Universidad Carlos III de Madrid

Escuela Técnica Superior

Ingeniería Técnica de Telecomunicación: Sonido e Imagen

PROYECTO FIN DE CARRERA

Diseño y solución de red para la integración de Centros de Datos

Autor: **Mercedes Hernán García-Prieto**

Tutor: **Dr. D. Manuel Urueña Pascual**

Índice de contenidos

RESUMEN

El presente proyecto contempla el diseño de una solución de interconexión de dos centros de procesado de datos (CPDs) con el objetivo de fusionar dos empresas a nivel de red, a las que llamaremos empresa C y empresa G.

Se trata de dos entidades bancarias que por motivos políticos y económicos han acordado unirse dando lugar a una sola entidad. Para que esto sea posible las dos empresas, mediante mutuo acuerdo, han contratado a un grupo de ingenieros integradores de redes expertos en el campo y capaces de ofrecer una solución totalmente transparente para el cliente.

El integrador ofrece en esta memoria una solución técnica cuyo objetivo es unir los núcleos de la red de forma que los usuarios de una empresa tengan acceso a los recursos y/o servicios de la otra empresa, y viceversa. De esta manera, se logra unir ambas empresas como si fuese una sola.

Aprovechando esta solución de red, el integrador resolverá problemas presentes en las dos empresas ofreciendo mejores alternativas para garantizar mayor seguridad, escalabilidad y eficiencia en la red. Paralelamente se aprovecharán mejor los recursos existentes, como el equipamiento y las tecnologías, para el mismo objetivo; ofrecer una solución altamente potente y escalable tanto a corto como a largo plazo.

Tanto la definición como la solución de este proyecto han sido ideados por la autora del mismo, no habiéndose basado para ello en ningún escenario real.

ABSTRACT

This project involves the design of a solution for interconnection of two data centers (CPDs) in order to merge the network of the two companies, called company C and company G.

Both companies are two financial entities that for political and economic reasons have agreed together resulting in a single entity. To make this merger possible, both companies have hired a group of expert network integrators who are able to provide a fully transparent solution for the customer.

The integrator provides in this project a technical solution which aims to unite the Core of the network so that users have access to company resources and / or services of the other company, and vice versa. Thus, it is possible to unite the two companies as if it were a single.

Taking advantage of this network solution, the integrator will solve actual problems in both companies offering better alternatives to ensure greater security, scalability and network efficiency. In parallel, existing resources will be taken on advantage, such as equipment and technologies, and all of that for the same purpose; to offer a powerful and highly scalable solution.

Both the definition and the solution of this project have been designed by the author himself, without basing herself on any real scenario.

1. INTRODUCCIÓN

El constante crecimiento de las redes *ethernet* obliga a las grandes infraestructuras a evolucionar en un mundo en constante demanda y competitividad. El motivo principal que empuja a realizar este cambio es principalmente la lista de requisitos de los clientes, los cuales optan siempre por una mejoría en la rápida y eficaz respuesta de los servicios.

Estas prestaciones que deben ofrecer nunca serán suficientes sin un núcleo fuerte que sea capaz de hacer llegar la información lo más rápido posible, evitando en mayor medida problema muy comunes hoy en día como los cuellos de botella, o pérdidas de tráfico de datos, voz o multimedia. Y es en este punto en el cual se centrará el proyecto, ofreciendo una solución que se adecúe lo más posible a los requisitos de cliente, tanto a nivel de servicio como a nivel económico.

El Centro de Datos o CPD es la parte principal de una arquitectura de red donde se origina o pasa la mayor parte del tráfico de datos. Por este motivo, es importante que el centro de datos esté bien protegido ante ataques maliciosos, tanto desde dentro de la red (intranet) como fuera de ella (internet).

Hay que tener en cuenta que en muchos casos, y en función de las necesidades del cliente, el centro de datos puede crecer año tras año, por lo que siempre es recomendable realizar un diseño de arquitectura altamente escalable.

La alta disponibilidad o redundancia es un punto clave a tener en cuenta en un diseño de red, ya que, en caso contrario, nos podemos encontrar con pérdidas o aislamientos de tráfico que no desearíamos en ningún caso. Es por esto que desde los puntos remotos hasta el centro de datos, como el núcleo o el enrutador ISP, debe haber redundancia de conexiones.

Este proyecto presenta una solución a aquellos problemas tan comunes que existen hoy en día en los centros de datos aprovechando el objetivo principal del mismo; la integración o unión de tres centros de datos.

La empresa C, entidad financiera y situada en Getafe, consta de un edificio de varias plantas con un número escaso de usuarios, y una arquitectura de red bastante simple pero con muchos puntos críticos de red, causando lentitud y pérdidas de tráfico. Aprovechando que la empresa G va a adquirir a la empresa C, se realizará un estudio de todas las criticidades que presenta para mejorarla a la vez que se diseña y se realiza la integración de las dos empresas.

La empresa G, como ya se ha mencionado, a adquirirá económicamente la empresa C. La empresa G presenta dos edificios principales los cuales contienen a su vez un centro de proceso de datos (CPD) cada uno; uno está situado en Alcobendas, y el otro está situado en Leganés. Estos dos edificios albergan una cantidad muy grande de usuarios y servidores a lo largo de las plantas y los CPDs. Además, tiene una red de sucursales u oficinas situadas a lo largo de la Península que, durante el proceso de integración con la empresa C, seguirá existiendo tal y como existe ahora sin modificar su infraestructura de red actual.

En el siguiente apartado se comentarán los objetivos principales que realizará el integrador de red estableciendo unas pautas durante todo el proceso del proyecto.

1.1. Objetivos

Los objetivos principales de este proyecto son:

- Realizar un análisis técnico en profundidad de ambas infraestructuras según las necesidades del cliente tanto a nivel económico como técnico.

- Detectar problemas que puedan estar afectando a la seguridad de las dos empresas y corregirlos en base a mejorar la disponibilidad y rendimiento de los servicios.

- Analizar los puntos fuertes de las dos empresas para tenerlos en cuenta de cara a la integración y aprovechar sus funciones durante la solución.

- Establecer la interconexión entre los centros de datos con el equipamiento acordado y expuesto, realizando todas aquellas tareas que permitan las comunicaciones entre todos los servicios de las dos infraestructuras.

1.2 Estructura de la Memoria

En primer lugar, el proyecto describirá cada una de las tecnologías que actualmente se están implementando o que se implementarán durante el proceso del proyecto y serán aquellas que, de acuerdo a lo hablado entre integrador y cliente, tengan un papel importante en todo el proceso, ya que claramente es inviable describir cada una de las tecnologías y/o protocolos que componen una infraestructura de red tan grande como la que presentamos. Todo esto se describirá en el apartado 2 de la memoria.

En segundo lugar se describirá, en el apartado 3, la arquitectura actual de las dos empresas. De esta manera se tendrá una visión clara del estado actual que presentan, determinando así sus puntos de fallo y mejora, analizándolos en el apartado 4.

El apartado 5 será el que contendrá la solución del proyecto, ofreciendo en detalle una solución lo más clara y sencilla posible. Esta solución se basará en integrar los tres CPDs que componen las dos empresas, unificando cada uno de sus protocolos de red y aprovechando al máximo el hardware y software que las dos empresas utilizan actualmente.

Una vez explicada la solución de integración, se dará una planificación del proyecto en el apartado 6, teniendo en cuenta las jornadas y recursos que formarán parte del presupuesto, expuesto al final del mismo.

Finalmente, se concluirá el proyecto en el apartado 7 ofreciendo los trabajos que se han de tener en cuenta en el futuro para mejorar la seguridad y la eficacia de las nuevas empresas integradas.

2. DESCRIPCIÓN DE LAS TECNOLOGÍAS UTILIZADAS

Este apartado describirá los protocolos de red de nivel 2 y nivel 3 que juegan un papel importante en la solución del proyecto.

2.1. Tecnologías Ethernet

Ethernet se utiliza masivamente en las empresas y especialmente en sus CPDs. Esta sección repasará este tipo de tecnologías avanzadas que están empleando actualmente las empresas C y G, o que se planean usar para su interconexión.

2.1.1 IEEE 802.1Q

IEEE 802.1Q es un mecanismo de etiquetado de las tramas *ethernet*, mediante el cual se inserta una etiqueta de campo de 4 bytes en la trama *ethernet* original entre la dirección de *Origen* y el campo *Type/Lenght* (ver Figura 1). A causa de esta inserción, el campo FCS de la trama modificada se recalcula.

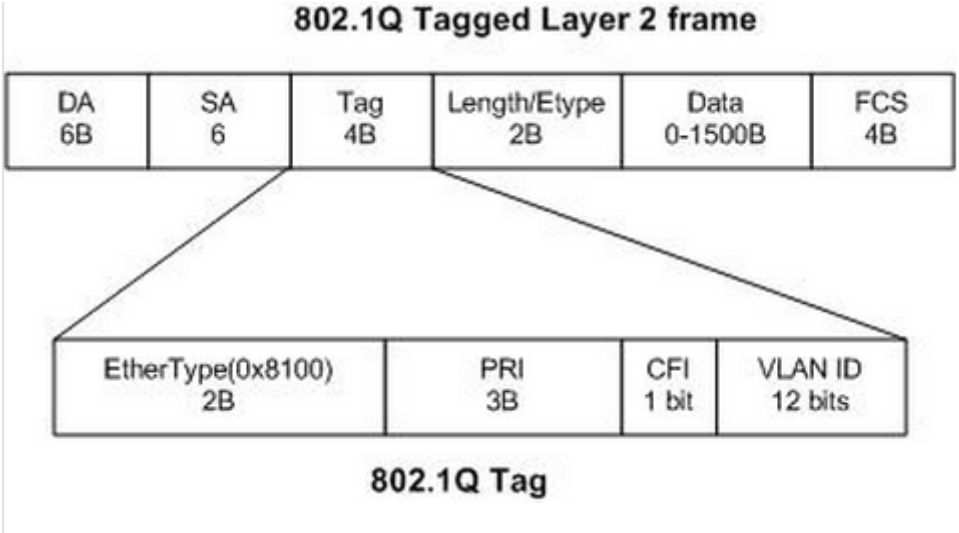


Figura 1: Trama 802.1Q. [Cisco Certified Networking Associate (CCNA)]

La Figura 1 muestra la expansión del campo *Tag 802.1Q* completo. La expansión incluye los acrónimos de los campos y el número de bytes de cada campo.

Descripción de los campos

***Tag Protocol Identifier* (TPID):** El TPID es un campo de 16 bits. Se le asigna un valor de 0x8100 para identificar que se trata de una trama IEEE 802.1Q.

***Priority*:** También conocido como prioridad de usuario, este campo de 3 bits hace referencia a la prioridad IEEE 802.1p. Este campo se usa para priorizar el tráfico. El campo puede representar hasta 8 niveles de Calidad de Servicio (QoS) cuyos valores están comprendidos entre 0 y 7.

***Canonical Format Indicator* (CFI)**: El CFI es un campo de 1 bit. Si el valor de este campo es 1, la dirección MAC está en formato no canónica. Si el valor es 0, la dirección MAC está en formato canónico (eg. *Ethernet, Token Ring*).

***VLAN Identifier* (VID):** El identificador VLAN es un campo de 12 bits. Este identifica explícitamente la VLAN a la cual pertenece la trama. El campo puede tener un valor entre 0 y 4095.

La etiqueta 802.1Q ocupa 4 bytes. Por lo tanto, la trama *Ethernet* resultante puede llegar a medir 1522 bytes. El tamaño mínimo de una trama *Ethernet* con etiquetado 802.1Q son 68 bytes.

2.1.2 Link Aggregation Control Protocol (LACP)

Es un subcomponente de IEEE 802.3ad que ayuda a aumentar el ancho de banda entre equipos interconectados utilizando varios enlaces en paralelo, entre los que se reparte la carga de manera transparente. Además, gracias a ella se pueden crear enlaces redundantes proporcionando una mayor disponibilidad. Se pueden agrupar hasta 16 enlaces con LACP. De esta manera, si falla uno de los enlaces, la carga se distribuirá entre el resto de enlaces, y esto será prácticamente transparente para el usuario. Es decir, que no se producirá ningún corte en la red. Esto es debido a que LACP utiliza mecanismos que son capaces de detectar rápidamente la caída de los enlaces físicos y redireccionar el tráfico al resto de enlaces.

Para que estos mecanismos funcionen, los enlaces deben transmitir activamente paquetes especiales usados en este protocolo, llamados *packet data units* (PDUs), que son los que se encargan (activa o pasivamente) de recuperar las caídas de enlaces. La función activa de LACP consiste en que cada cierto tiempo se envían PDUs de sincronización entre ambos extremos para determinar posibles caídas de agregaciones. Un enlace LACP pasivo se activa únicamente cuando se quieren enviar PDUs en caso de caída de enlace.

Como ya se ha mencionado, se pueden utilizar hasta 16 enlaces formando una agregación, aunque no todos pueden estar activos a la vez, sino que solo se permiten hasta 8 enlaces activos. El conmutador que menor prioridad de sistema tenga (un valor de prioridad de 2 bytes seguido de una dirección MAC) será el que decida qué enlaces se pondrán como activos y cuáles no. Los otros enlaces se mantienen en *standby*, y serán activados en caso de que alguno de los activos falle.

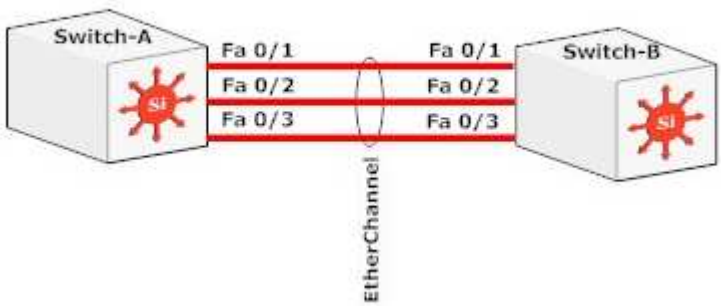


Figura 2: Configuración de *switches* utilizando LACP. [http://www.computerfreetips.com/cisco-router/EtherChannel-LACP-Protocol.html]

2.1.3 Agregación de conmutadores *ethernet*

En esta sección se explicará en qué consiste esta característica tan usada hoy en día, poniendo como ejemplo los equipos de Juniper y Cisco, ya que ambas tecnologías se utilizarán a lo largo de la integración (*Virtual Chassis* para los equipos Juniper y *Stackwise* para los equipos Cisco).

Utilizando esta característica resulta posible crear un conmutador virtual agrupando varios conmutadores independientes. Su objetivo es aprovechar los beneficios de conexión en un *rack* con las de un chasis tradicional. La Figura 3 muestra la disposición de varios equipos conectados como un chasis virtual.

Figura 3: Ejemplo de Chasis Virtual en equipos Juniper.
[http://i2.wp.com/www.ebrahma.com/wp-content/uploads/2015/08/Recover-the-password-and-configuration.jpg]

El hecho de poder extender la densidad de puertos de un conmutador permite a los servicios informáticos cubrir las necesidades futuras de evolución de su red bajo demanda. Cuando se forma un chasis virtual, este actúa como una única unidad lógica. Los administradores de red supervisan y gestionan este equipamiento como si fuese de un único chasis físico.

Para formar un chasis virtual se configura una única IP como parte de la configuración inicial. Una vez que se configura esta IP, los equipos se unen para formar parte del grupo junto con el *master*, utilizando la misma IP, por lo que esta tecnología también es muy útil a la hora de ahorrar direccionamiento, ya que solamente se utiliza una IP por cada grupo virtual formado.

Juniper Virtual Chassis

Tomando el ejemplo de la Figura 4, cada equipo dispone de su propio plano de control y de datos (o *forwarding)* independientes del resto.

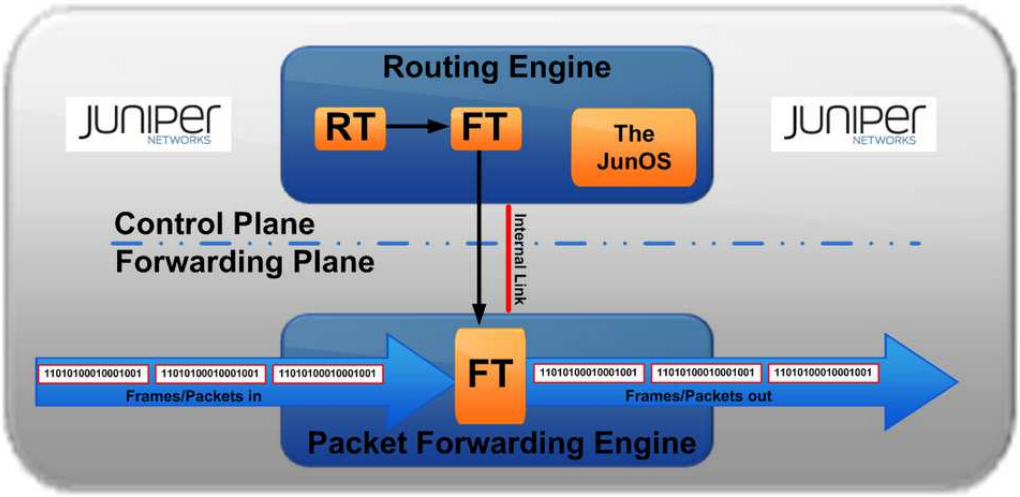


Figura 4: Planos de Control y Datos en la tecnología Juniper. [www.juniper.net]

Al crear el chasis virtual, lo que se hace realmente es fusionar los cinco planos de *forwarding* en uno solo. Esta fusión se efectúa conectando los *Packet Forwarding Engine (PFE),* dejando como activo un único elemento de control o *Routing Engine (RE).* Además, es posible aumentar capacidad al *backplane* añadiendo vínculos adicionales entre los conmutadores tal como se muestra en la Figura 5.

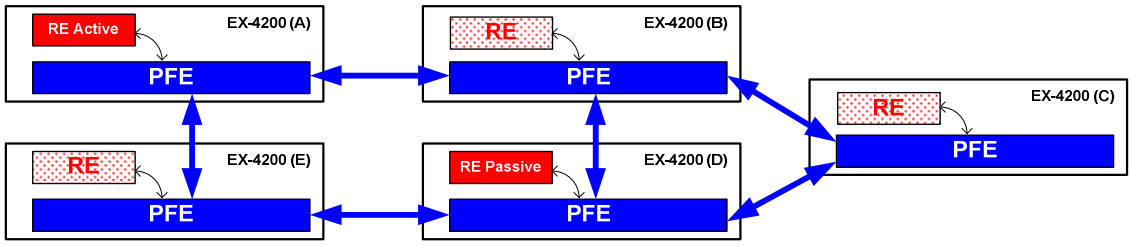


Figura 5: Mejora del rendimiento en un Chasis Virtual. [Juniper Networks Certified Associate (JNCIA)]

Existen dos formas de unir cada conmutador independiente en el chasis virtual:

Puerto *Virtual Chasis Port (*VCP): Situados en la parte trasera del conmutador, cada uno de estos puertos dispone de una capacidad de 64 Gbps *full-dúplex* a una distancia máxima de 3 metros. Cada conmutador dispone de dos puertos VCP.

Puerto de fibra: Dependiendo del modelo del fabricante, la mayoría de los conmutadores disponen de cuatro o más puertos de fibra, pudiéndose utilizar 1 ó 2 de ellos para formar el chasis virtual, dando cada uno un ancho de banda de hasta 10Gbps.

Cuando se forma un chasis virtual de Juniper, cada conmutador asume un rol, que puede ser uno de estos tres:

- ***re0***: Es el plano de control activo (o *master*) y es el que controla toda la parte de gestión y encaminamiento de paquetes. También controla las tarjetas en línea, enviando las instrucciones de *forwarding*.

- ***re1***: Es el plano de control pasivo, cuya labor es la de sincronizar todos los estados de encaminamiento y de tablas de *forwarding* cada cierto tiempo con el *re0*, ya que actúa de *backup* en caso de pérdida con el *re0*.

- **Tarjetas de línea:** Estas tarjetas están encargas del *reenvío* de paquetes, albergando las tablas de *forwarding* locales enviadas por la *re0*.

En el caso de un *Chasis Virtual* de *N* miembros, a dos de ellos se les asignan los papeles de *re0* (*master*) y *re1* (*backup*), y el resto de los miembros permanecen como simples tarjetas de línea.

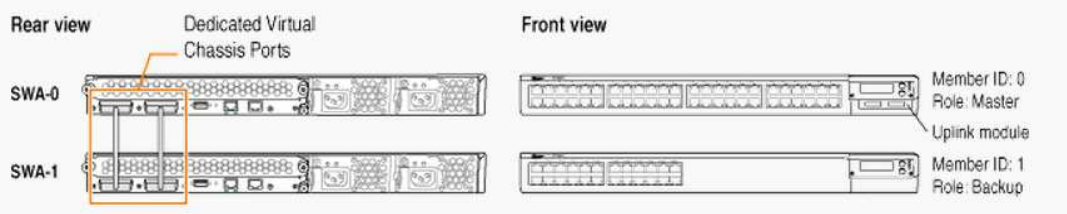


Figura 6: Representación de los distintos módulos de un chasis Juniper. www.juniper.net.

Cisco StackWise

Esta característica de los conmutadores Cisco mantiene las funcionalidades muy parecidas a las de la tecnología *Virtual Chassis* de Juniper.

Aunque la terminología difiera entre los fabricantes, la funcionalidad es la misma. Es decir, en ambos casos, un *stack*, pila o chasis virtual se comporta de la misma manera apilando varios conmutadores físicos para dar lugar a uno virtual.

Mientras que en Juniper se pueden utilizar hasta diez equipos formando un chasis virtual, en Cisco sólo se permiten hasta nueve equipos.

La información de configuración y de *routing* es compartida por todos los conmutadores del *stack*, creando una sola unidad. Los *switches* se pueden añadir o quitar en caliente sin que afecte a su rendimiento.

Al igual que en los equipos Juniper, los Cisco también utilizan cables de *stacking* especiales de fabricante, que crean caminos bidireccionales cerrados en bucle. A través de esta conexión, se actualizan constantemente la información de *routing* y la topología de red. La interconexión del *stack*, se gestiona mediante una sola unidad, llamada *master*, y que es elegida previamente.

Los conmutadores se conectan físicamente en cascada. Si se rompe uno de los cables de *stacking*, el ancho de banda se reducirá a la mitad de su capacidad. Cuando el *stack* (o la pila)

detecta problemas de tráfico, los mecanismos de recuperación son capaces de realizar el *failover* en microsegundos, para así conmutar todo el tráfico al otro camino que queda activo.

Elección del master

La función principal del *master* es la de crear y actualizar automáticamente toda la conmutación y las tablas de encaminamiento del *stack*. Cualquier miembro del *stack* puede ser *master*. Después de un reinicio o una nueva instalación, comienza un proceso de elección entre los conmutadores de la pila, basándose en el siguiente criterio de selección. Este criterio se utiliza en ambas tecnologías:

1. **Prioridad de usuario**: El administrador de red puede elegir manualmente qué conmutador será el *master*.
2. **Prioridad de Software y Hardware**: El conmutador con la versión más reciente será el *master* del *stack*.
3. **Configuración por defecto**: Si un conmutador ya tiene configuración de *stacking*, tomará preferencia sobre otros conmutadores que no han sido configurados previamente.
4. ***Uptime***: El conmutador que lleve más tiempo encendido será seleccionado *master*.
5. **Dirección MAC**: Cada conmutador informa de su MAC a cada uno de los miembros con los que va a hacer *stacking*, y será elegido aquel que tenga la menor dirección de MAC.

Figura 7: Ejemplo de *StackWise* en equipos Cisco.
[https://supportforums.cisco.com/discussion/11247516/3750g-and-multi-chassis-link-aggregation]

2.1.4 *Cisco Virtual Switching System* (VSS)

El concepto de *Virtual Switching System* (VSS) consiste en agrupar más de un *Switch* 6500 en un dominio virtual, que permite a los equipos funcionar en conjunto y ser administrados como uno solo. Anteriormente la redundancia de Catalyst 6500 se producía configurando dos equipos funcionando individualmente y corriendo STP y VRRP entre ellos.

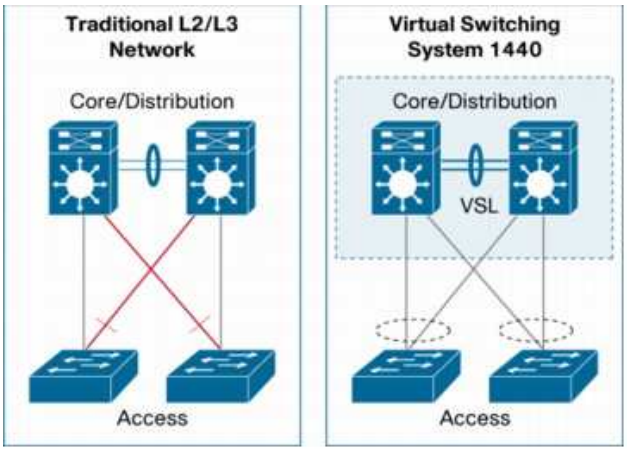


Figura 8: evolución de los *uplinks* con VSS.
[http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod_qas0900aecd806ed74b.html]

Con VSS se elimina la necesidad de tener STP y protocolos como VRRP, ya que, aunque a nivel físico son dos chasis, se comportan como uno solo a nivel lógico. Uno de los chasis asumirá el rol de plano de control activo y el otro mantendrá su plano de control en *standby (*o respaldo), pero ambos chasis son capaces de hacer *forwarding* de paquetes simultáneamente. Esto permite que se pueda configurar sólo una dirección IP en los servicios y que la misma sea mantenida por el equipo que tenga activo el plano de control.

La configuración de VSS se realiza uniendo los dos chasis mediante los puertos de 10Gbps de la supervisora. Sobre estos puertos se establece un protocolo específico LMP (*link management protocol*) que se encarga de gestionar el funcionamiento del VSS (*virtual switching system*).

La utilización de ambos puertos proporciona mayor ancho de banda y redundancia de puertos en caso de caída de uno de ellos. El *Switch Fabric* del chasis (*hardware* encargado del *forwarding* de paquetes) se encuentra localizado en la propia supervisora. Si ocurriera un problema grave en la supervisora y esta quedara inutilizable, el chasis entero quedaría inutilizado, conmutando al otro equipo.

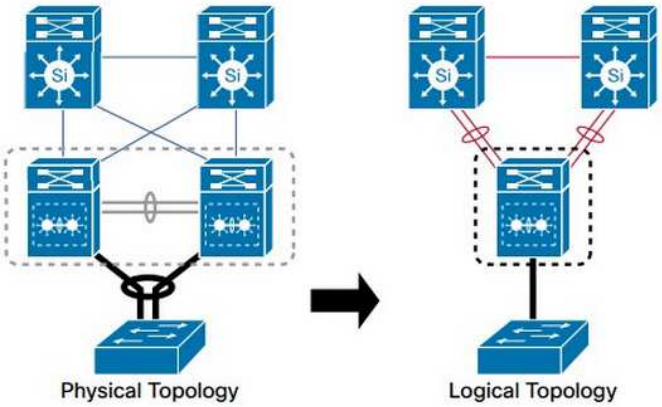


Figura 9: Topología Física y Lógica con VSS. [https://supportforums.cisco.com/document/124626/virtual-switching-system-vss-configuration-cisco-4500-series-switches]

Las principales diferencias entre esta funcionalidad y *Cisco Stackwise* es el tipo y la cantidad que se puede utilizar en cada una. VSS únicamente es compatible con la familia de equipos Cisco *Catalyst* 4500 y 6500/6800 y se usan dos del mismo modelo en cada *chasis virtual*. La tecnología S*tackwise* se utiliza en los *Catalyst* 2960, 3750, 3650 y 3850 y se pueden utilizar hasta nueve equipos del mismo modelo en la misma pila.

2.1.5 *Multichassis Ethernet Channel* (MEC)

Una de las principales ventajas del VSS es poder realizar una conexión desde un conmutador a un puerto de cada uno de los chasis Cat6500 para dar redundancia de enlaces. Al comportarse los dos chasis como uno solo, estos dos enlaces se pueden agregar para formar un *EtherChannel* o agregado, eliminando la necesidad de establecer el protocolo *Spanning-tree* y permitiendo que ambos enlaces estén activos simultáneamente.

A este tipo de conexión se le denomina MEC (*Multichassis EtherChannel*), que es la capacidad de un VSS para realizar *EtherChannels* desde cualquier tarjeta de puertos en cualquiera de los chasis hacia un conmutador o enrutador ajeno, ya sean equipos individuales o equipos formando *Chasis Virtual* o *Stacking.*

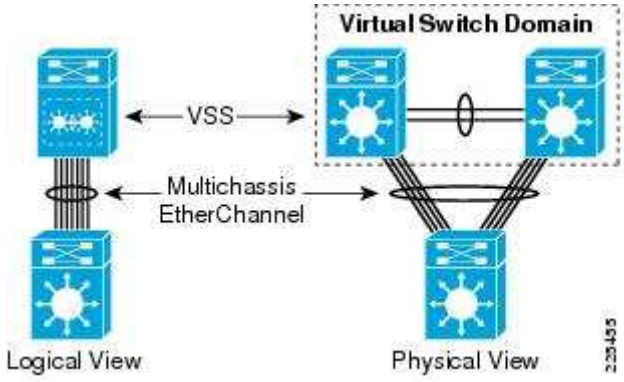


Figura 10: Ejemplo de MEC en topología VSS.
[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/vssdc_integrate.html]

En caso de caída de uno de los enlaces que componen el MEC, el envío o *forwarding* de paquetes se continuará realizando por el resto de miembros del MEC, sin importar qué chasis tenga el plano de *forwarding* activo.

Se utilizará MEC para conectar la capa de distribución con la capa de Core y con la capa de acceso. Todas las pilas de conmutadores o *switches* que se conecten a la capa de distribución y lleven redundancia de equipos, deben conectarse utilizando MEC para proporcionarles redundancia de caminos.

2.2. *Virtual Router Redundancy Protocol (VRRP)*

Virtual Router Redundancy (VRRP) es un protocolo estándar diseñado para eliminar el punto único de fallo que existe cuando en una red sólo hay un dispositivo actuando como ruta por defecto o *puerta de enlace (DG).* Cuando un grupo de enrutadores están configurados con VRRP, el protocolo asigna dinámicamente a uno de ellos la función de enrutador virtual. El enrutador que controla la IP asociada al enrutador virtual será el *master* del grupo VRRP.

Por tanto, una vez formado el grupo VRRP, tendremos una IP virtual asociada al grupo, que será la que haga de *DG* para los dispositivos de la LAN. Se asignará también un enrutador de respaldo que asumirá el rol de DG si el enrutador que actúa como *master* deja de estar disponible. De esta manera, se aporta redundancia a nivel de puerta de enlace.

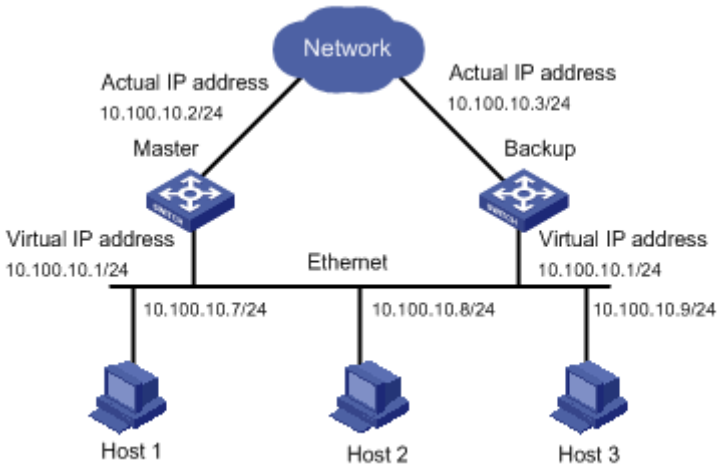


Figura 11: Esquema de red con VRRP. [http://www.h3c.com/portal/Technical_Support___Documents]

Al enrutador virtual se le asocia una dirección IP virtual y una MAC virtual. Esta IP y esta MAC nunca cambian independientemente del enrutador físico que el protocolo escoja como *master*.

El enrutador *master* envía periódicamente a la dirección IP 224.0.0.18 un paquete de datos en el cual indica su estado. Si durante un tiempo determinado los enrutadores de respaldo dejan de recibir este paquete del enrutador *master*, entonces el enrutador de respaldo de mayor prioridad pasa a convertirse en el nuevo enrutador *master* del enrutador virtual, es decir, todo el tráfico hacia Internet será encaminado por un enrutador de *backup* reconvertido en enrutador *master*.

2.3. *Multiprotocol Label Switching* (MPLS)

En una red IP tradicional, un enrutador reenvía los paquetes de una interfaz de entrada a una interfaz de salida, además de actualizar la información de encaminamiento. Para enviar los paquetes, se debe examinar la cabecera de cada paquete IP. Estas dos funciones de envío y encaminamiento tienen lugar en cada salto que realiza un paquete, para todos los paquetes que atraviesan la red. Además, cada enrutador de la red necesita aprender todas las rutas que se intercambia con el resto mediante el protocolo de encaminamiento, y esto reduce la eficiencia de los enrutadores a nivel de hardware, memoria, tiempo de convergencia del protocolo de encaminamiento, etc.

Para solventar estos problemas del IP tradicional, *Multiprotocol Label Switching* (MPLS) ofrece una solución que se basa en realizar las funciones de encaminamiento únicamente en los equipos exteriores del dominio MPLS, de tal manera que en el interior de ese dominio no sea necesario realizar funciones de encaminamiento, sino sólo de reenvío mediante la consulta de unas etiquetas añadidas a cada paquete en el momento de entrada al dominio.

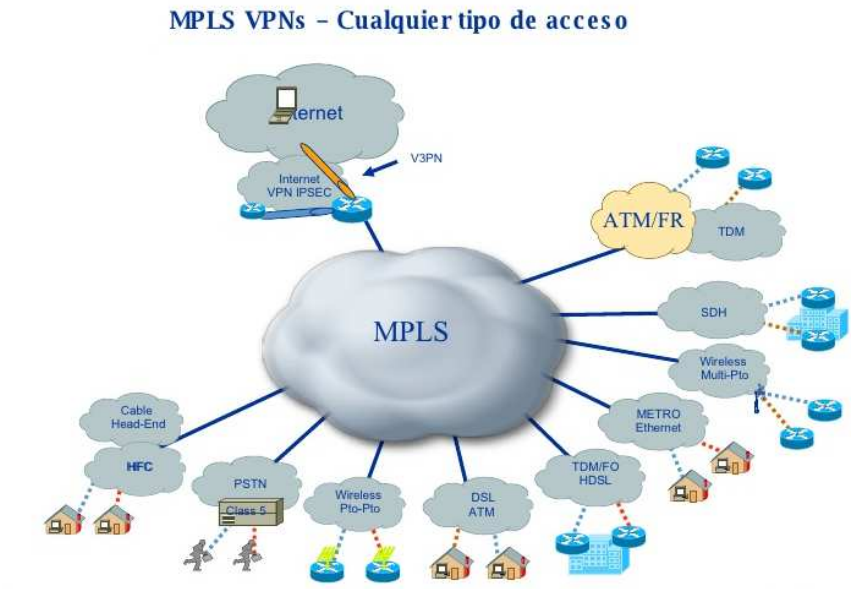


Figura 12: Arquitectura de un proveedor con MPLS. [es.slideshare.net]

Las ventajas que ofrece esta tecnología MPLS/IP son:

- Es una solución que proporciona garantías de calidad de servicio (QoS – *Quality of Service*) extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones e implementar ingeniería de tráfico a una red global que soporte todo tipo de tráfico.

- Una de las principales ventajas de una red única es la simplificación que representa una única administración. Sobre esta red se pueden crear tantas redes virtuales como sea necesario.

- Proporciona un modelo de servicios "inteligentes", ya que se puede utilizar MPLS para crear redes privadas virtuales (VPNs).

- La red MPLS permite realizar VPNs de nivel 2 y 3, además de la posibilidad de realizar ingeniería de tráfico sobre ellas.

- Las IP VPN, además de aislamiento y seguridad, evitan la complejidad de las VPNs basadas en IPSec de nivel 2 (conexiones punto a punto, configuración manual, problemas de crecimiento, problemas de gestión de la QoS).

2.3.1 Terminología MPLS

Un *label switch router* (o LSR) es un enrutador en una red MPLS capaz de identificar etiquetas y de enviar y recibir los paquetes etiquetados. Existen tres tipos de LSRs (Figura 13):

- ***Ingress LSRs***: Es el enrutador de la red MPLS que recibe un paquete que aún no ha sido etiquetado. Le inserta una etiqueta –*push*– en la cabecera del paquete y lo envía a través de la red MPLS.
- ***Egress LSRs***: Es el enrutador de la red MPLS que quita la etiqueta y lo envía a la red de datos fuera de la red MPLS –*pop*–. Tanto los *ingress LSRs* como los *egress LSRs* se denominan *edge LSRs* o *LSRs* de borde.
- ***Intermediate LSRs***: Es el enrutador de la red MPLS que recibe paquetes etiquetados entrantes y, tras realizar una serie de operaciones –*swap*–, envía el paquete etiquetado por el camino más definido.

Un LSR puede realizar estos tres tipos de operaciones: *pop, push* o *swap.*

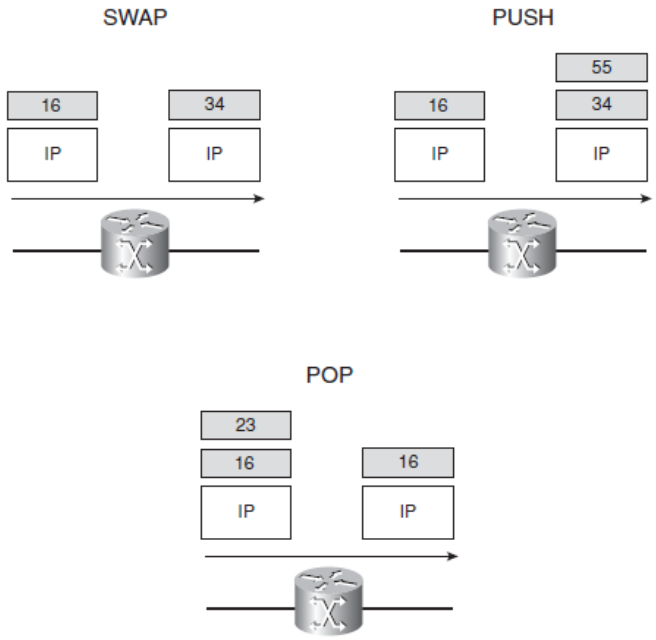


Figura 13: Operaciones con etiquetas MPLS. [*Cisco MPLS Fundamentals*].

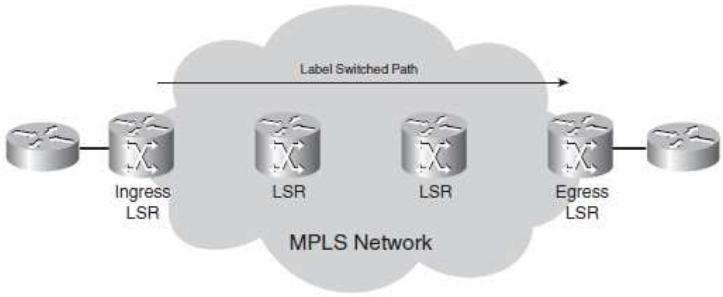


Figura 14: Tipos de LSR en una topología MPLS. [*Cisco MPLS Fundamentals]*

- ***Label Switched Path* (LSP):** Se denomina así a cada uno de los caminos unidireccionales que se establecen mediante conmutación de etiquetas en un dominio MPLS. Es el camino que siguen los paquetes por una red MPLS y que pertenecen a una misma FEC. Se forman desde el destino hacia el origen.

- ***Forwarding Equivalent Class* (FEC)**: Es un grupo de paquetes que se envían a lo largo del mismo camino de la red MPLS y se tratan de la misma manera en cuanto a la forma de realizar el *forwarding*. Todos los paquetes que pertenecen al mismo FEC tienen la misma etiqueta. El enrutador que decide qué paquete pertenece a qué FEC es el *Ingress LSR*, ya que es el que clasifica las etiquetas y los paquetes. Existen diversas formas para clasificar los paquetes en FEC, basándose en el prefijo de destino, en el grupo *multicast*, etc.

- ***Etiqueta* (Label):** Es un identificador corto de longitud fija que se usa para identificar un FEC. Es importante destacar que las etiquetas sólo tienen significado local en cada interfaz. Contienen un campo de 32 bits, de los cuales los primeros 20 pertenece a la propia etiqueta. Los bits EXP se utilizan para implementar Calidad de Servicio (QoS). El bit de S indica si la etiqueta es la primera o no del *stack* (conjunto de etiquetas que se encuentran en la cabecera del paquete). El resto de bits que componen la cabecera MPLS es el TTL típico también en los paquetes IP, que decrementa en uno cada salto que da para evitar que los paquetes recorran la red indefinidamente en caso de bucle (figura 15).

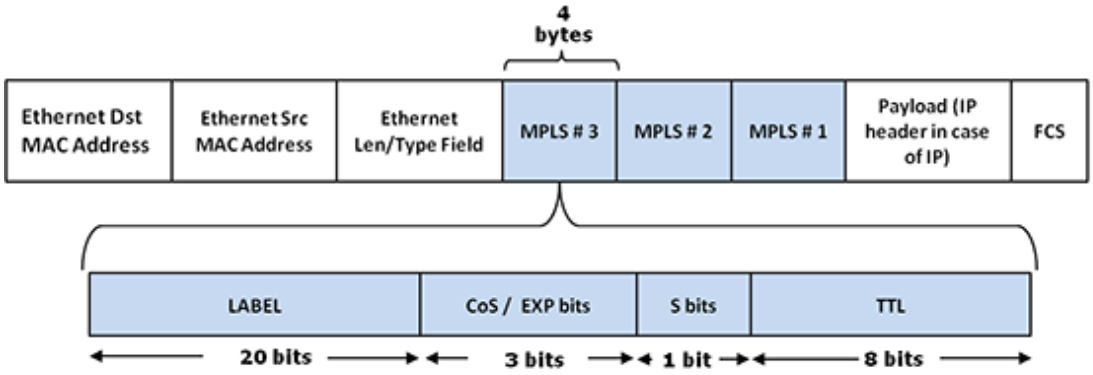


Figura 15: Estructura etiqu0eta MPLS.
[http://www.gl.com/optical-and-ethernet-testing-packetexpert.html]

2.3.2 Funcionamiento MPLS

MPLS se basa en la utilización de etiquetas, que son identificadores cortos de longitud fija y de significado local. Dichas etiquetas se añaden a los paquetes en la entrada del dominio MPLS por parte de los *Ingress LSRs* o enrutadores de entrada al dominio MPLS.

Las etiquetas serán conmutadas e intercambiadas dentro de dicho dominio por los *Core LSRs* para finalmente ser retiradas a la salida del dominio por parte del *egress LSR* entregando el paquete original. Las etiquetas se añaden de manera general entre las cabeceras de nivel 2 y 3.

Las etiquetas permiten identificar un FEC (*Forwarding Equivalente Class*), agrupación de paquetes que comparten los mismos atributos (dirección destino, VPN…) y/o requieren el mismo servicio (*multicast*, QoS). El FEC se asigna en el momento que el paquete entra en la red, y todos los paquetes que forman parte del FEC siguen un mismo LSP (*Label Switched Path*), a través de varios *LSRs*.

El funcionamiento de la red MPLS se basa en:

- Construir tablas de encaminamiento mediante los algoritmos de encaminamiento, interiores (como OSPF, RIP, ISIS) o exteriores (como eBGP).
- Definir los LSP o caminos MPLS. Estos caminos se construyen mediante tablas de intercambio de etiquetas entre los *LSRs* P adyacentes. Las etiquetas se distribuyen mediante un protocolo de distribución de etiquetas. Se puede utilizar el protocolo denominado *Label Distribution Protocol* (LDP), definido específicamente para MPLS u otros protocolos como RSVP o CR-LDP (*Constraint-Based Routing LDP*).
- Una vez que los *LSRs* conocen las etiquetas que deben utilizar para conmutar los paquetes de un determinado FEC, el dominio MPLS en cuestión está en condiciones de cursar el tráfico de la siguiente manera:

    1. Cuando un paquete entra en el dominio MPLS a través del *LSR* de entrada, éste lo etiqueta y lo envía por la ruta LSP correspondiente al FEC identificado por la etiqueta.
    2. Los *LSRs* reenvían los paquetes a través del LSP mediante el intercambio de etiquetas (*swaps*), no siendo necesario procesar las cabeceras del protocolo de la capa de red (normalmente la cabecera IP).
    3. El *LSR* de salida del dominio MPLS extrae la etiqueta y envía el paquete al nodo destino, CE.

2.3.3 *Virtual Private Networks* (VPNs)

Una Red Privada Virtual (VPN), como la misma palabra indica, se trata de una red privada, normalmente en un dominio público, que se utiliza para conectar diferentes redes de clientes de forma segura.

En nuestro caso, las VPNs se consideran redes independientes, cada una se guarda su tabla de encaminamiento, y dan servicio a los diferentes sitios de cliente, siendo estos, en nuestro caso, los CPDs.

La interconexión de diferentes sitios de un mismo cliente se realiza mediante VPNs. Las VPNs creadas pueden ser de nivel 2 o de nivel 3.

Terminología VPN

- ***Customer Edge Router*** (CE): Son los equipos de cliente que se conectan con el proveedor mediante un protocolo de capa 2 típicamente *ethernet*. En caso de que el cliente necesite conectividad de nivel 3 con otros CE, será necesario disponer de un protocolo de encaminamiento, estático o dinámico, entre el CE y el equipo del Proveedor (PE).

- ***Provider Edge Router*** (PE): También denominado enrutador de borde, se ubica en la red de proveedor y está conectado directamente con los equipos de cliente CE; además, los PE se comunican con otros PE de la red de proveedor empleando MPLS.

- ***Provider Router*** (P): Es un nodo interno de un dominio MPLS que conmuta los paquetes entre PE solamente en función de la etiqueta. Estos equipos no disponen de ninguna información acerca de las VPNs de cliente, ya que su función se basa únicamente en conocer la etiqueta de entrada para saber por dónde enviarla.

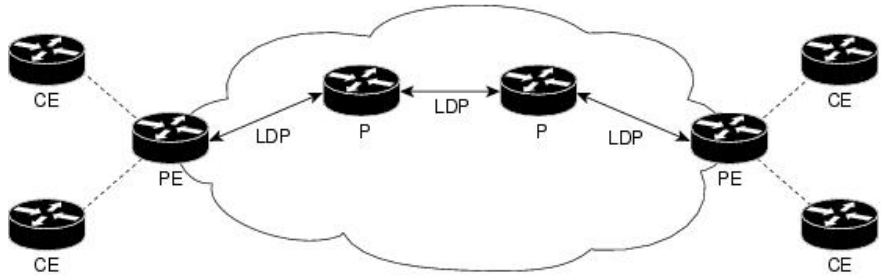


Figura 16: Diferentes roles en una topología MPLS VPN. [*Cisco MPLS Fundamentals]*

- ***VPN Routing & Fordwarding Table*** **(VRF):** En una VPN de nivel 3 cada PE mantiene tablas de *routing* independientes para cada cliente; a estas tablas de cliente se les denomina VRF. Cuando un CE anuncia sus redes al PE que tiene directamente conectado, este actualiza dichas redes en la correspondiente tabla VRF del cliente y envía una actualización a los PE remotos que disponen de esa misma VRF. Los PEs remotos, a su vez, envían esa actualización al CE localmente conectado al cliente.

- ***VPN Fordwarding Table*** **(VFT):** En una VPN de nivel 2 cada PE crea una tabla VFT para cada cliente CE que tiene conectado. Las tablas VFT contienen información que identifican el tipo de conexión entre CE-PE, el tipo de encapsulación, la *interface* lógica, el identificador local de sitio, información de las etiquetas MPLS e información de las ubicaciones remotas conectadas a través del LSP.

- ***VPN Conection Table*** **(VCT):** La información contenida en cada VFT se transmite entre los PE mediante VCT. Cada VCT es parte de la información contenida en la VFT de un cliente. El intercambio de VCT permite a los PEs enviar las tramas de capa 2 recibidas del CE al correspondiente PE remoto.

La Figura 17 muestra gráficamente cómo el PE de una infraestrcutura con MPLS realiza las funciones de *IP switching* hacia el acceso y *MPLS Switching* hacia el Core o nube MPLS. Es este tipo de *router* quien añade la primera etiqueta MPLS al paquete IP para enviarla a la nube MPLS, o bien el que quita la última etiqueta del paquete IP para enviarla al acceso de su LAN.

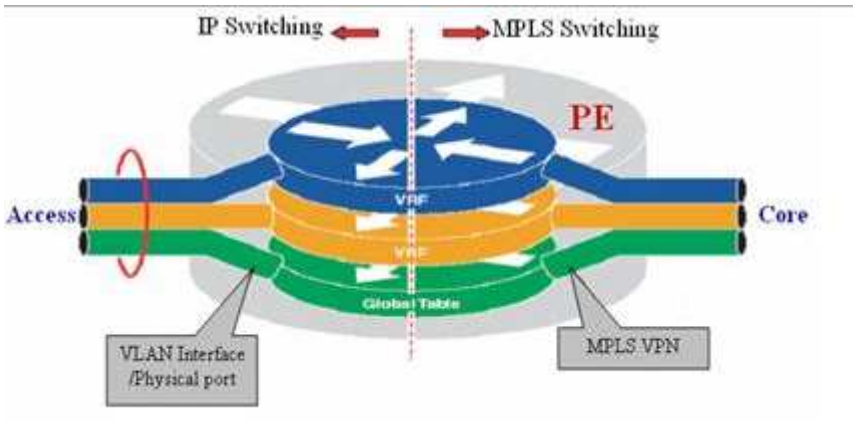


Figura 17: Funciones en un PE en una topología MPLS VPN. [juniper.net]

VPNs de Nivel 3: VRFs

Cada enrutador PE genera una instancia de encaminamiento para cada VPN de cada cliente. De esta forma, el nivel 3 de cada uno de ellos queda totalmente independizado del resto. Entre el enrutador PE del proveedor y el enrutador CE del cliente puede correr cualquier tipo de protocolo de encaminamiento (ej. OSPF, RIP, BGP, rutas estáticas).

Dentro del núcleo de la red MPLS, la información de un mismo "cliente" o "Servicio" es intercambiada mediante extensiones del protocolo BGP (MP-iBGP), denominadas NLRI (*Network Layer Reachability Information*). Este intercambio de NLRI requiere que se establezcan sesiones iBGP entre todos los PEs de la red.

De esta forma se tiene que entre dos PEs se emplea un LSP que llevará tráfico de dos tipos, genérico e información de una VPN. Esto se consigue añadiendo otro nivel de etiquetas:

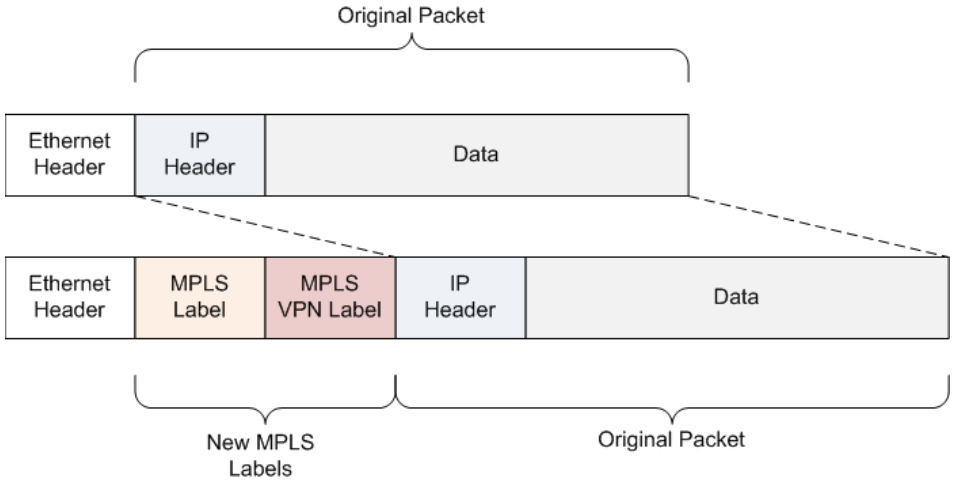


Figura 18: Formato de un paquete viajando por un *Label Switched Path (*LSP). [*infrastructureadventures.com]*

- El primer nivel se denomina externo (*outer*) o *MPLS Label,* e indica cómo formar el camino LSP hasta llegar al PE remoto.
- El segundo nivel se denomina interno (*inner*) o MPLS VPN *Label* e indica al PE remoto a qué VPN pertenece el paquete.

Para separar las VPNs de distintos “clientes” o “Servicios”, es necesario disponer de una tabla de rutas independiente o VRF por “Servicio”; se utiliza el atributo denominado **Route-Distinguisher (RD)** que identifica cada prefijo o ruta de cliente.

Este atributo, junto con el prefijo IPv4, forman un prefijo VPNv4 que se anuncia a los PE de la red mediante MP-iBGP. Permite, además, el solapamiento de direcciones IP entre distintas VPNs.

Este atributo es un valor de 8-bytes que se puede definir con el siguiente formato: ***route-distinguisher*** *(as-number: number | ip-address: number)*

Para distribuir prefijos VPNv4 (RD+IP) a través de los PEs o, dicho de otra forma, para identificar las rutas que pertenecen a una determinada tabla de rutas (VRF), se emplea el ***router-target***. El *router -target* es una comunidad extendida de BGP que se adjunta en todos anuncios de cada tabla VRF. Cuando el PE recibe un anuncio, comprueba que la comunidad recibida coincide con la comunidad local de su VRF y entonces actualiza las rutas en la tabla VRF. Para que estos anuncios sean posibles es necesario tener sesiones iBGP entre todos los PEs.

VPNs de Nivel 2: VPLS

El Servicio de LAN Privada Virtual (VPLS) es una forma de proporcionar comunicación *Ethernet* multipunto a multipunto sobre redes IP/MPLS. La tecnología VPLS (*Virtual Private LAN Swithing*) permite que todos los elementos conectados a la red en diferentes sedes se vean como si estuviesen en la misma LAN, sin necesidad de conversiones a otros protocolos, ya que el transporte es Ethernet extremo a extremo. Desde el lado del acceso se trata como si fuese un único dominio de difusión.

En una VPN de nivel 2, el tráfico de nivel 2 de la capa de distribución o CE (*Customer Edge*) es transportado por la red IP/MPLS a través de un túnel o instancia VPLS. Las instancias VPLS se establecen entre los PEs (*Provider Edges*) y en ellas se indican los puertos que pertenecen a la instancia, que serán los puertos que den conexión entre el CE y el PE. Los PEs no necesitan conocer las tablas de encaminamiento de la capa de distribución o CE, únicamente deben identificar el túnel o instancias VPLS por donde se debe enviar el tráfico.

VPLS puede trabajar en un entorno de VPNs p2n (1 a n), a diferencia de un entorno en nivel 2 que solo puede trabajar con VPNs p2p (1 a 1). De este modo, un paquete originado en un CE puede transmitirse por *broadcast* a todos los PEs que participan en el dominio VPLS.

La figura 19 muestra un esquema de VPLS sobre una red IP/MPLS.

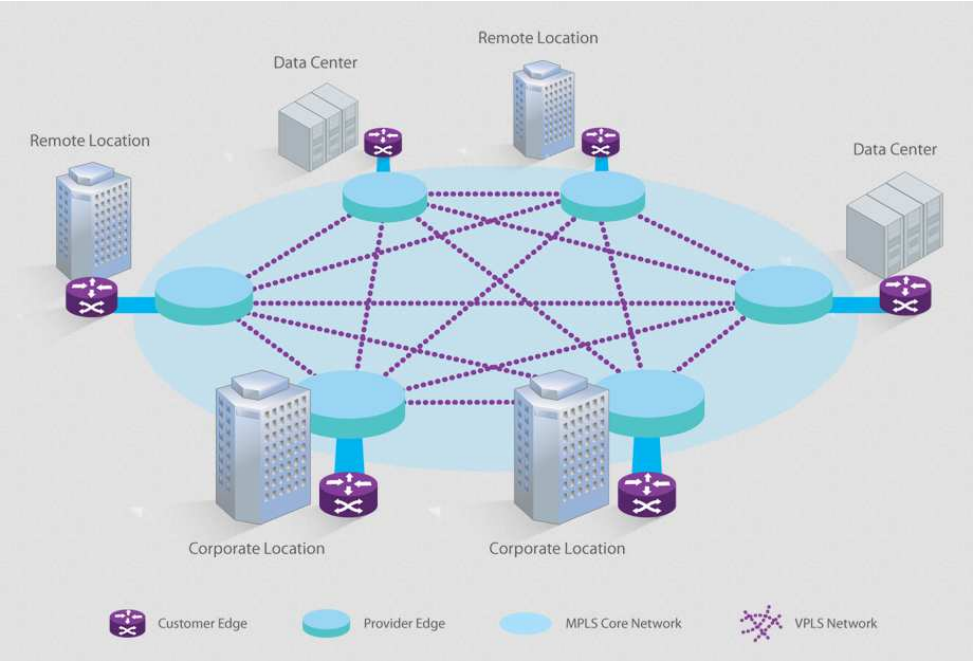


Figura 19: Ejemplo de VPLS sobre una red MPLS. [www.xo.com]

VPLS permite que los PEs implicados controlen el tráfico, ya que pueden identificar el destino de ese paquete VPLS sin tener que enviarlo a todos los PEs que componen la red VPLS. Los equipos de un entorno VPLS realizan las siguientes funciones:

- *Switch* de Acceso (CE):
  - Se conecta con el PE a través de un enlace *Ethernet.*
  - Puede tener Nivel 3 (IP, IPX, SNA).
  - Requiere una conexión lógica por VPLS.
- *Provider Edge routers* (PE), también llamado VE (VPLS *edge* o de borde):
  - Mantiene información relacionada con la VPN.
  - Se encarga de aprender las direcciones MAC del cliente.
  - Intercambia la Información de las VPNs relacionadas con otros PEs mediante MP-BGP.
  - Utiliza MPLS LSPs para transportar tráfico entre los PEs.
- *Provider routes* (P):
  - Conmutan tráfico de la VPN de forma transparente sobre el LSP establecido.
  - No mantienen información relacionada con la VPN.

Las instancias VPLS, en lugar de construir y anunciar tablas rutas como las VPN de nivel 3, construyen tablas de conmutación denominadas VFT y anuncian tablas de conexión de VPN VCT.

Las tablas VFT contienen información sobre el *site* ID, las interfaces lógicas, encapsulación, etiquetas, etc. Estas tablas se anuncian mediante VCT, que son un subconjunto de información de la VFT. Al igual que el anuncio de rutas de las VPN de nivel 3, las VCTs se anuncian al resto de PEs mediante MP-iBPG, por lo que todos los PEs han de tener sesiones iBGP entre ellos.

VPLS *multihoming*

VPLS *multihoming* permite conectar un equipo de cliente a varios PEs para proporcionar conectividad redundante, al tiempo que se evita la formación de bucles de nivel 2 en la red MPLS. Un sitio VPLS *multihoming* conectado a dos o más enrutadores PE proporciona conectividad redundante en caso de caída del enlace entre el CE y PE, o en caso de caída del enrutador PE.

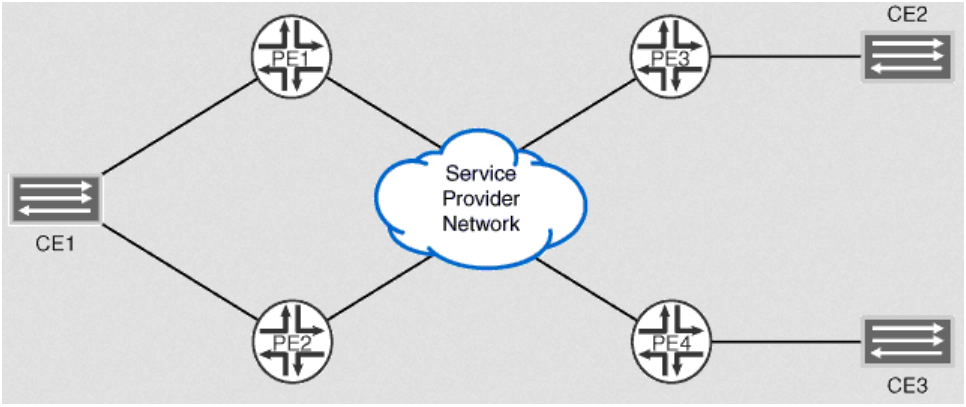


Figura 20: Ejemplo de VPLS *Multihoming*. [Cisco MPLS Fundamentals]

Si los enrutadores PEs están conectados al mismo sitio y se les asigna el mismo identificador de dispositivo VPLS Edge (VE) (*multihoming*), entonces se construye una topología libre de bucles utilizando un mecanismo de encaminamiento de selección de rutas como BGP. Cuando un equipo BGP recibe dos anuncios NLRI (*network layer reachability information*) equivalentes, se aplica el criterio normal de selección de ruta como, por ejemplo, la preferencia local y AS path para determinar qué NLRI elegir, de forma que se selecciona sólo uno.

Debido a que los enrutadores PE seleccionan solo uno de los anuncios NLRI, se establece un *pseudowire* solo con uno de los enrutadores PE remotos, el enrutador PE que originó el anuncio ganador. Esto evita la creación de múltiples caminos en la red entre sitios VPLS, evitando la formación de bucles de nivel 2. Si el PE elegido falla, todos los enrutadores PE de la red cambiarán automáticamente al PE de respaldo y se establecerá el *pseudowire* a través del PE de respaldo.

Dos *VPLS NLRIs* se consideran equivalentes desde una perspectiva de selección de ruta si los siguientes campos son los mismos:

- *Route distinguisher*
- *VE device identifier*
- *VE block offset*

Si a dos enrutadores PE se les asigna el mismo identificador de dispositivo VPLS *Edge* (VE) en un determinado entorno VPLS, también deberán anunciar el mismo tamaño de bloque VE para un determinado VE *offset*.

VPLS Multihoming es una característica muy interesante a la hora de evitar propagar *spanning-tree* a lo largo de CPDs o *sites* remotas.

2.4. *Open Shortest Path First* (OSPF)

Open Shortest Path First (OSPF) es un protocolo de encaminamiento de estado de enlace desarrollado para redes IP por el IETF a modo de *Interior Gateway Protocol* (IGP). Utiliza el algoritmo de Dijkstra para calcular la ruta más corta posible, construyendo una base de datos, idéntica en todos los enrutadores de la zona.

Se trata del sucesor natural del protocolo RIP, capaz de utilizar *Classless Inter-Domain Routing* (CIDR) utilizando máscaras de subred de tamaño variable (VLSM). Existen, además, varias versiones, como OSPFv3, que soporta IPv6.

2.4.1 Tipos de paquetes OSPF

Existen cinco tipos de paquetes OSPF:

- ***Hello:*** Se utiliza para establecer adyacencias entre enrutadores. Se envía un paquete *multicast* 224.0.0.5 por todas las interfaces del enrutador y *unicast* en los enlaces virtuales. Una vez establecidas las adyacencias, se enviarán este tipo de paquetes para el mantenimiento de las mismas, en el que se envía un listado de los vecinos del enrutador y la relación que mantiene con cada uno de ellos. Estos paquetes de mantenimiento se enviarán con un intervalo de 10 segundos en redes LAN.
- ***Database description*:** Sirve para sincronizar las bases de datos entre enrutadores.
- ***Link-state request*:** Pide registros específicos de estado de enlace de enrutador a enrutador.
- ***Link-state update**:* Manda registros de estado de enlace que fueron solicitados.
- ***Link-state acknowledgement**:* Son acuses de recibo de paquetes OSPF.

Una red OSPF se puede descomponer en varias regiones (áreas). Existe un área central o de *backbone*, a la que se conectarán el resto de áreas. Normalmente los enrutadores forman enlaces punto a punto entre ellos, aunque para un mismo segmento *Ethernet*, se elegirá un enrutador designado (DR) y un enrutador designado de respaldo (BDR), con el fin de reducir el *tráfico* entre las adyacencias.

2.4.2 Tipos de enrutadores OSPF

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de enrutadores cuya información se puede resumir de cara al resto de la red. Un área es una unidad de encaminamiento; es decir, todos los enrutadores de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (*Link State Database*). De esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella.

Un enrutador OSPF clásico es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra (encaminamiento intra-área). Para el encaminamiento entre distintas áreas del AS (encaminamiento inter-área) y desde el AS hacia el exterior (encaminamiento exterior), OSPF utiliza enrutadores especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

- ***Router interior:*** Se encuentran dentro de un área**.**
- ***Router de backbone:*** Se trata de un enrutador interior situado en el área de *backbone* o área 0.
- ***Area Border Router (ABR):*** enrutador de frontera de área. Se sitúa entre dos o más áreas. Una de ellas debe ser el área 0.
- ***Autonomous System Boundary Router (ASBR):*** Viene dado por la redistribución de rutas de otros protocolos de encaminamiento. Se trata de un enrutador en la frontera entre OSPF y una red no OSPF. Pueden encaminar los paquetes fuera del sistema autónomo (AS) en el que se encuentran.

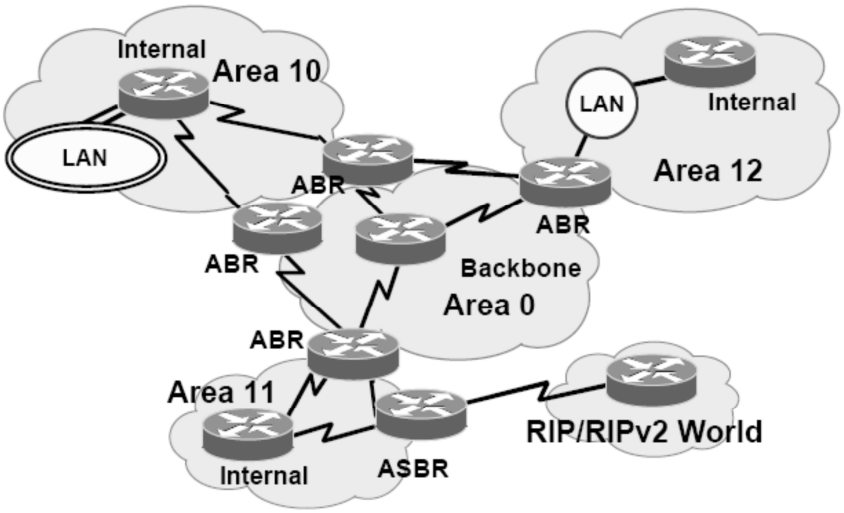


Figura 21: Enrutadores de OSPF. Recuperado de www.cisco.com

Del mismo modo, dentro de un segmento Ethernet, se pueden distinguir varios tipos de *routers* OSPF:

- ***Router Designado (DR):*** Llevará a cabo las tareas de envío y sincronización. El objetivo de que haya un enrutador designado es el de reducir el tráfico entre adyacencias.
- ***Router designado de respaldo (BDR):*** Se trata de un enrutador que sólo actuará en caso de que el DR principal falle.

Para elegir a un enrutador como enrutador designado se tendrá en cuenta la prioridad. Por defecto, la prioridad en OSPF es 1. El enrutador con un valor de prioridad más alto será elegido como DR. Si un enrutador tiene prioridad cero, no podrá ser elegido nunca como DR o BDR. En caso de que todos los enrutadores tengan la misma prioridad, se elegirá dependiendo del enrutador *ID*: número de 32 bits que identifica de manera única al enrutador dentro de un mismo sistema autónomo. Se elegirá como enrutador ID la dirección IP más alta de una interfaz activa o, en caso de tenerla, la dirección de *loopback*.

2.4.3 Tipos de áreas OSPF

OSPF distingue los siguientes tipos de áreas:

- ***Area Backbone***: También conocida como área cero, presente en cualquier red OSPF y es a la que deben estar conectadas el resto de áreas. Esta conexión se realizará mediante los ABRs.

- ***Area Stub***: Se trata de un área que no redistribuye rutas externas de otros protocolos que no sean OSPF. Si este tipo de enrutador necesita encaminar hacia otras redes fuera de la red OSPF, utilizará la ruta por defecto 0.0.0.0/0 para que sea enviada por el ABR hacia los demás enrutadores que forman el área *Stub.*

- ***Area not-so-stubby***: También conocida como NSSA, constituye un tipo de área *stub* que puede importar rutas externas de sistemas autónomos y enviarlas al *backbone*, pero no puede recibir rutas externas de sistemas autónomos desde el *backbone* u otras áreas.

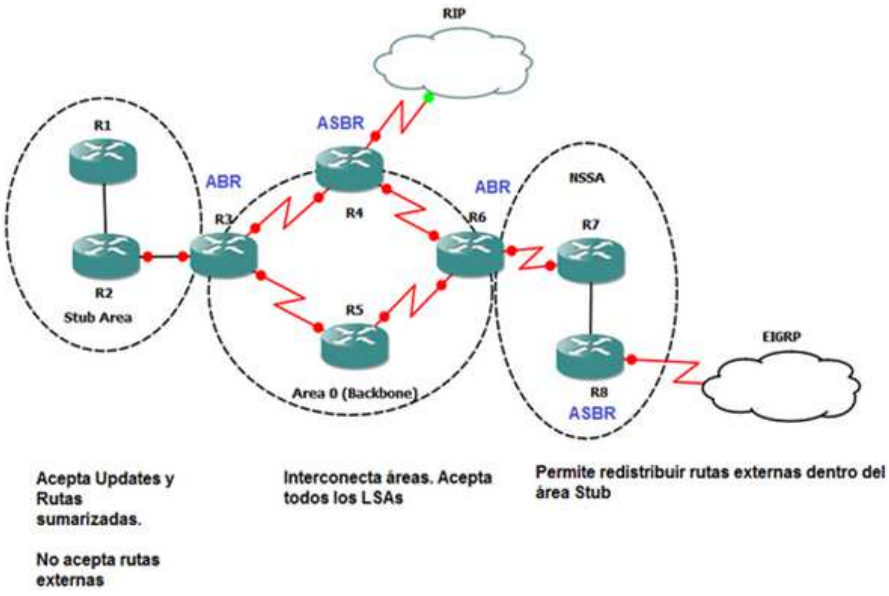


Figura 22: Ejemplo de enrutadores y áreas OSPF. [http://www.redescisco.net/v2/art/tipos-de-areas-en-ospf/]

Funcionamiento en redes punto a punto

En redes punto a punto, el enrutador detecta dinámicamente a sus vecinos enviando paquetes *Hello* con la dirección *multicast* 224.0.0.5. No existe concepto de DR o BDR. Los intervalos *Hello* y *Dead* son de 10 y 40 segundos, respectivamente.

Mantenimiento de la información de encaminamiento

Para el mantenimiento de la información de encaminamiento, cuando un enrutador detecta un cambio, realiza una multidifusión de un paquete LSU (*Link-state Update*) con la dirección 224.0.0.6.

El DR confirma la recepción del LSU e inunda la red con un LSU a la dirección *multicast* 224.0.0.5. El resto de enrutadores, al recibir el LSU, actualizan su base de datos.

2.5. Border Gateway Protocol (BGP)

BGP es un protocolo de encaminamiento entre dominios diseñado para proporcionar encaminamiento sin bucles entre organizaciones. BGP está diseñado para funcionar sobre un protocolo de transporte fiable; utiliza TCP (Puerto 179) como protocolo de transporte. El puerto de destino asignado es el 179, el puerto local será aleatorio.

BGP se utiliza principalmente para conectar una red local a una red externa, por ejemplo a Internet o para conectarse con otras organizaciones. Cuando se conecta a organizaciones externas, se crean sesiones externas de BGP (eBGP). A pesar de que BGP se conoce como un *External Gateway Protocol* (EGP), muchas redes de una organización se vuelven tan complejas que BGP se emplea para simplificar la red interna de la organización. Los pares BGP dentro de una misma organización intercambian información de encaminamiento a través de sesiones de BGP interno (iBGP).

BGP utiliza un algoritmo de encaminamiento de *path-vector* para intercambiar información de red con lo demás dispositivos que hablan BGP. La información se intercambia entre pares BGP mediante actualizaciones de encaminamiento. La información intercambiada contiene el número de red, atributos del camino y la lista de sistemas autónomos que la ruta debe atravesar para alcanzar la red de destino. Esta lista aparece contenida en el atributo *AS-path*. BGP previene bucles descartando cualquier actualización de *routing* que contenga el número de sistema autónomo local, ya que esto indica que la ruta ya ha atravesado el sistema autónomo y, por lo tanto, se ha generado un bucle. El algoritmo *path-vector* de BGPs resulta de una combinación de los algoritmos de vector-distancia y de detección de bucles.

BGP selecciona un único camino por defecto como camino óptimo para una red o nodo /destino. El algoritmo de selección de ruta analiza los atributos del camino para determinar qué ruta está instalada como camino óptimo en la tabla de rutas de BGP**.** La selección del camino BGP también puede venir determinado a través de políticas de configuración BGP.

2.5.1 Sistemas Autónomos

Un sistema autónomo es una red controlada por una única entidad administrativa. Los sistemas autónomos en BGP se utilizan para dividir redes externas en dominios de encaminamiento individuales, donde las políticas de encaminamiento son aplicadas a nivel local. Esta organización simplifica la administración de dominios de encaminamiento y la configuración de una política de encaminamiento coherente. La configuración de políticas de encaminamiento coherentes es importante para permitir que BGP pueda procesar las rutas asociadas a las redes de destino de manera eficiente.

Cada dominio de encaminamiento puede soportar múltiples protocolos de encaminamiento. Sin embargo, cada protocolo de encaminamiento se administra de manera independiente. Otros protocolos de encaminamiento pueden intercambiar información de encaminamiento de manera dinámica a través de la distribución BGP. Distintos sistemas autónomos de BGP intercambian dinámicamente información de encaminamiento mediante sesiones de *peer* eBGP. Los *peers* dentro de un mismo sistema autónomo intercambian información mediante sesiones IBGP.

3. ARQUITECTURA DE RED ACTUAL

En este apartado se describirán las arquitecturas de red de las dos empresas, dando a conocer, en primer lugar, la infraestructura física y el equipamiento utilizados y, posteriormente, describiendo la parte lógica y los protocolos de red que las componen.

3.1. EMPRESA C

A continuación se describirá el conexionado físico actual de los equipos de red de la empresa C situada en Getafe, tanto a nivel físico como lógico. Cabe reseñar que la empresa, constituida únicamente por un edificio, consta de 140 empleados y está diseñada para que cualquier usuario tenga libre acceso tanto a la granja de servidores como a Internet.

3.1.1 Diseño físico

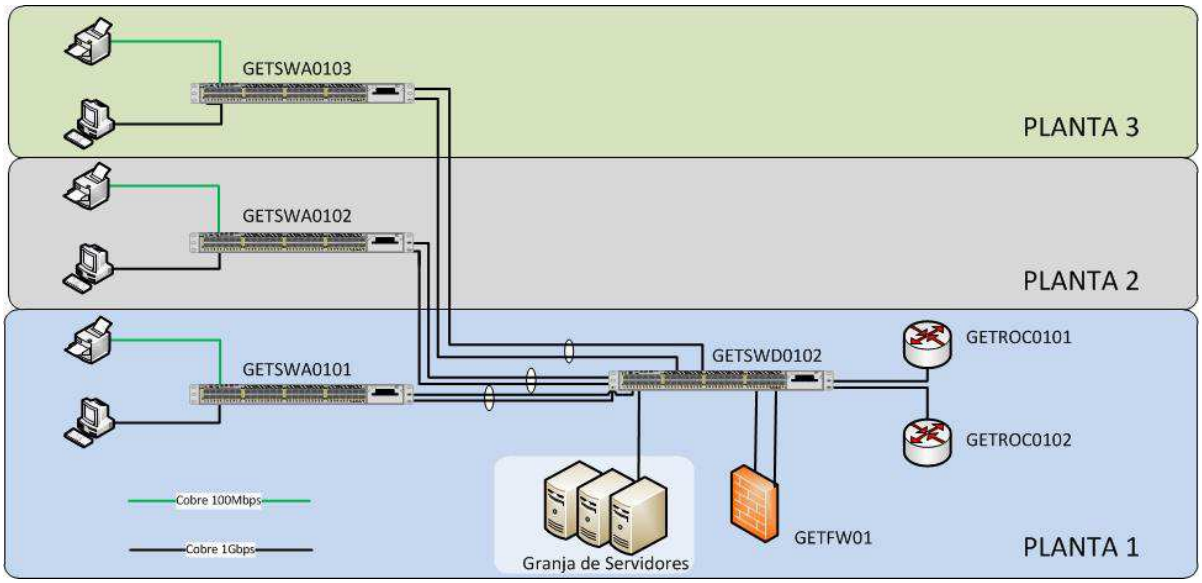


Figura 23: Esquema físico de Empresa C

Capa de acceso

Esta capa está distribuida a lo largo de los cuartos técnicos instalados en cada una de las tres plantas de que consta el edificio, repartiendo por igual la conectividad tanto de los usuarios y teléfonos como de las impresoras. Cada planta contiene uno o varios (según las necesidades) *switches* Catalyst 3750X de 48 puertos PoE (*Power over Ethernet*) para proporcionar alimentación a los teléfonos *VoIP*. Ofrecen 100Mbps a las impresoras y hasta 1Gbps a cada usuario.

Para conectar los teléfonos en cada puesto de usuario no es necesario una toma independiente de red, sino que se sitúan entre el puerto del conmutador y el PC del usuario, ya que el conmutador es capaz de proporcionar tanto tráfico multimedia como alimentación al teléfono gracias a la tecnología PoE. La Figura 24 muestra un diseño típico de un puesto de usuario:

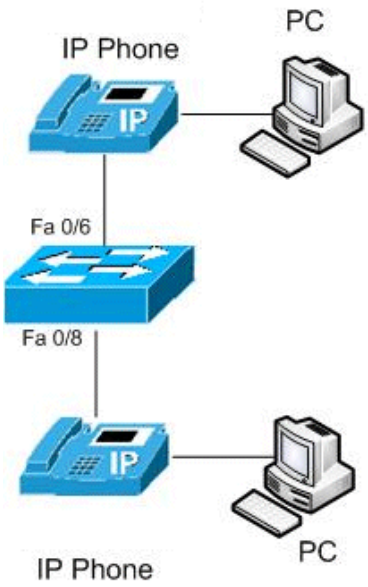


Figura 24: Ejemplo de conexión con teléfono PoE+PC.
[http://www.cisco.com/c/dam/en/us/support/docs/switches/catalyst-2950-series-switches/113260-voice-vlan-01.gif]

Una configuración típica que presentan los equipos de acceso para dar conectividad a puestos de usuario es la siguiente:

```
interface GigabitEthernet1/0/1
description UsuarioPc+ telefono
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan add 10,30
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
spanning-tree bpduguard enable
end
```

Capa de distribución

La distribución o agregación está formada por un *switch* Cisco Catalyst 3750X-48T, siendo el punto central de conectividad entre usuarios, impresoras y servidores con el *Core*. También da conectividad al *firewall* y a los enrutadores de salida a Internet.

Núcleo

Para ofrecer acceso a Internet, la empresa tiene contratado un servicio de operador que consta de dos Cisco de la serie 800 conectados a la distribución en cobre y ofreciendo un ancho de banda de 1Gbps por cada enlace. El proveedor de Internet contratado en la empresa C conecta a su CPD mediante una red utilizando la tecnología MPLS.

A continuación, la Tabla 1 muestra las conexiones entre las capas de acceso y distribución:

GETSWD0102	GETSWA0101	GETSWA0201	GETSWA0103	GETFW01
gi1/0/1	gi1/0/47			
gi2/0/1	gi1/0/48			
gi1/0/2		gi1/0/47		
gi2/0/2		gi1/0/48		
gi1/0/3			gi1/0/47	
gi2/0/3			gi1/0/48	
gi1/0/48				Port1
gi2/0/48				Port2

Tabla 1: Conexionado físico entre el acceso y la distribución de la empresa C

Conectado directamente a la distribución mediante varios enlaces de 1Gbps que describiremos en el siguiente apartado, la empresa C gestiona un *firewall* que utiliza políticas para aceptar o denegar tráfico entrante o saliente, ya sea por IP, por puerto, o ambos. Por defecto utiliza la política "denegar", es decir, todo está denegado excepto lo que se habilite explícitamente por sus administradores.

3.1.2 Diseño lógico

Teniendo en cuenta que el edificio tiene una capacidad para 140 usuarios, actualmente se utiliza direccionamiento privado de clase B para servidores y de clase C para el resto de elementos de red, quedando de la siguiente forma:

- 2 VLANs de usuarios distribuidas entre las tres plantas; suficientes para dar servicio a 140 usuarios, ya que cada VLAN corresponde a un direccionamiento de clase C y, por tanto, es capaz de dar conectividad a 254 usuarios.
- 2 VLANs de voz para dar conectividad a los teléfonos IP de los usuarios.
- 1 VLAN dedicada a la granja de servidores.
- 1 VLAN para gestionar los equipos de red.
- 1 VLAN dedicada a dar conectividad hacia el exterior, FW-*routers*.

La tabla 2 muestra la distribución y direccionamiento de cada subred o VLAN:

	DIRECCIONAMIENTO	VLAN ID	PLANTA
VLAN DE GESTIÓN	10.10.50.0/24	50	1, 2, 3
VLAN "DATOS_1"	10.10.10.0/24	10	1
VLAN "DATOS_2"	10.10.11.0/24	11	2, 3
VLAN "VOZ_1"	10.10.30.0/24	30	1
VLAN "VOZ_2"	10.10.31.0/24	31	2, 3
SERVIDORES	172.16.3.0/24	40	1, 2, 3
INTERNET	192.168.1.0/24	1	1

Tabla 2: Distribución del direccionamiento IP / VLANes por planta de la empresa C

La VLAN de gestión fue creada para que los administradores de la LAN pudieran acceder en remoto a cada uno de los equipos de la red y así poder gestionar la electrónica. Se trata de una gestión en banda, lo cual quiere decir que no es independiente al resto de tráfico existente en la red y la VLAN se extiende por los mismos troncales por los que se extienden el resto de VLANes.

El resto de VLANes fueron diseñadas para una arquitectura mediante encaminamiento inter-VLAN. Esto quiere decir que el FW actúa de nivel 3 para todas las VLANes, siendo el punto central de encaminamiento para el tráfico entre distintas VLANes (o subredes). Además, el firewall al ser la puerta de enlace (o *Default Gateway – DG)*, tendrá configurado el *DHCP relay* hacia la red de servidores, con el que tiene conectividad directa de N2 y conecta con el servidor DHCP que se encuentra en la granja. Este servidor DHCP instalado en un Windows Server 2003, se eliminará en la integración, ya que otro servidor se encargará de ofrecer el direccionamiento.

Actualmente, el servidor DHCP proporciona a cada uno de los PCs y teléfonos un direccionamiento de datos y otro de voz, siempre comprendidos en el rango 10.10.A.64-10.10.A.254. De esta manera, se dejan las IPs estáticas para las impresoras o para algún equipo de pruebas o de laboratorio. Esta casuística se mantendrá después de la integración.

Las VLANes de gestión y de servidores no utilizan DHCP, sino que son IPs estáticas configuradas por los administradores de red. Este método de configuración es recomendable para que las IPs de gestión y servidores siempre sean las mismas y no cambien dinámicamente. De no ser así, habría problemas para acceder a los elementos de la red, ya que podrían estar cambiando de IPs frecuentemente.

Cabe mencionar que ambos enrutadores utilizan HSRP para dar redundancia de puerta de enlace al FW, utilizando la IP virtual de HSRP para su función. Estos Cisco utilizan la tecnología ADSL 2+, que es capaz de ofrecer hasta un ancho de banda de 24Mbps de bajada y 1,2Mbps de subida.

Para el tráfico entrante o saliente a la empresa, el FW se encarga de NATear las IPs privadas de los usuarios y servidores, y envía el tráfico a su ruta por defecto, que en este caso es la IP virtual de los enrutadores Cisco del proveedor de internet.

El diseño lógico actual del edificio se muestra a continuación:

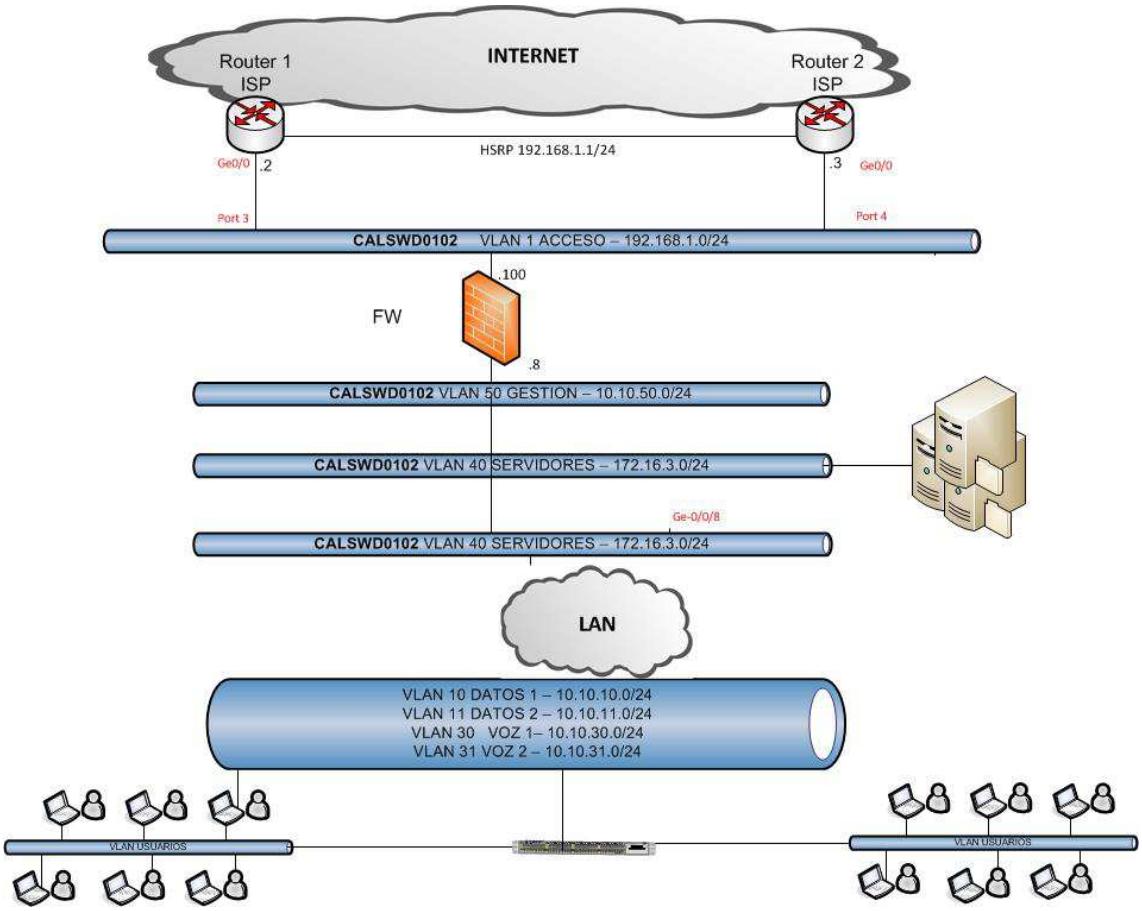


Figura 25: Esquema lógico de la empresa C

En este esquema se aprecia de manera muy sencilla cómo está extendido el nivel 2 entre las tres capas de la arquitectura de red. La IP del FW en cada subred corresponde con la que termina en .8 y éste es el *Default Gateway* de cada una de ellas, como ya se ha descrito.

3.2. EMPRESA G

Esta sección describe la infraestructura de red actual de la empresa G, tanto a nivel físico como lógico. Es importante destacar que esta empresa, una entidad financiera, consta de dos centros de datos de gran envergadura. Uno de ellos está situado a la afueras de Leganés, mientras que el otro está situado en Alcobendas, distando 30 kilómetros entre sí.

Además dispone de diversas oficinas o sucursales por toda la península que, mediante la red MPLS del operador, disponen de conectividad con los centros de datos de la empresa.

La arquitectura de red está dividida en varios entornos separados a nivel físico, cuyo punto en común es el núcleo, dedicado enteramente al nivel 3. Cada entorno constituye uno o más accesos, teniendo la distribución como punto común entre ellos.

En este proyecto se detallará aquella parte de la infraestructura que se vea afectada por la integración. El resto de equipamiento de red que se mantenga exactamente igual, tanto a nivel físico como lógico, quedará fuera del alcance de este proyecto.

3.2.1 Diseño físico

A continuación se detallará el esquema físico, dando como ejemplo en algunos casos uno de los CPDs, siempre teniendo en cuenta que ambos son completamente simétricos.

Núcleo

La capa de núcleo está formada por cuatro Juniper MX480, dos en cada centro de datos, interconectados a través de fibra oscura de 1Gbps por enlace mediante DWDMs gestionados por la empresa Fibernet.

Para la conexión de los equipos del núcleo con la capa de distribución de cada uno de los entornos, se dispone de tarjetas con interfaces a 1Gb configurados en LACP, por lo que ofrecen un ancho de banda de 2Gbps cada uno.

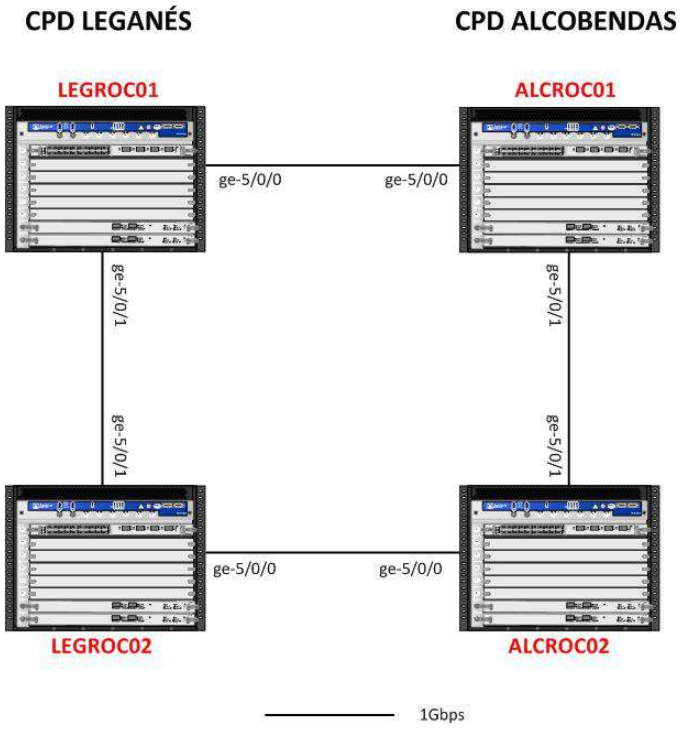


Figura 26: Esquema físico del núcleo de la empresa G

LEGROC01	LEGROC02	ALCROC01	ALCCROC02
ge-5/0/0	ge-5/0/0		
ge-5/0/1		ge-5/0/1	
	ge-5/0/0		ge-5/0/0
		ge-5/0/1	ge-5/0/1

Tabla 3: Interconexiones del núcleo de la empresa G

En el proceso de integración de las dos empresas se explicará con más detalle qué tarjetas se van a utilizar para dar este tipo de conectividad entre los centros de datos.

Capa de Distribución

La arquitectura de red de la empresa G está dividida en 4 entornos a nivel físico y lógico: Usuarios, Servidores, Oficinas e Internet. Estudiaremos cada uno de ellos, en detalle, más adelante.

Conectado al núcleo se encuentran dos equipos Catalyst 6509, utilizando la tecnología *Cisco Virtual Switching System (VSS)*. Estos equipos hacen de punto intermedio entre cada uno de los accesos de los distintos servicios y el núcleo. Se encarga de dividir cada uno de estos entornos a nivel físico y lógico y encaminar el tráfico hacia el núcleo. Para los enlaces agregados, también se utiliza la tecnología MEC para poder eliminar la dependencia de *Spanning-Tree*.

Además, existe otro equipo Catalyst 6504 que se encarga de hacer de distribución en el entorno de oficinas y encaminar el direccionamiento de estas hacia el núcleo.

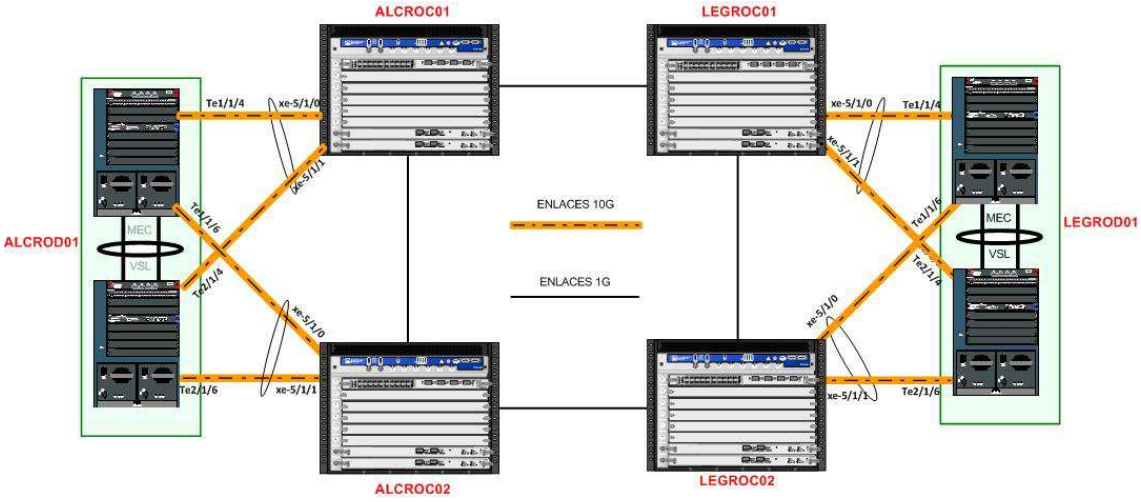


Figura 27: Interconexiones físicas entre el núcleo y la distribución de la empresa G

LEGROC01	LEGROC02	ALCROC01	ALCROC02	LEGROD01	ALCROD01
xe-5/1/0				Te1/1/4	
xe-5/1/1				Te2/1/4	
	xe-5/1/0			Te1/1/6	
	xe-5/1/1			Te2/1/6	
		xe-5/1/0			Te1/1/4
		xe-5/1/1			Te2/1/4
			xe-5/1/0		Te1/1/6
			xe-5/1/1		Te2/1/6

Tabla 4: Interconexiones entre el núcleo y la distribución de la empresa G

Todos los enlaces que componen esta capa son enlaces de 10Gbps, utilizando fibras entre ellos, y dando uso a la tecnología LACP entre los *uplinks*. Con esto, y añadiendo la tecnología VSS, se consigue redundancia tanto a nivel de equipo como a nivel de enlace, ofreciendo un ancho de banda de 20 Gbps por cada equipo de núcleo.

Para evitar bucles, *spanning-tree está* configurado en los CPDs, pero en este proyecto no se profundizará en ello, ya que en la solución se va a eliminar la dependencia de *spanning-tree* utilizando filtros en el núcleo.

Capa de Acceso

Como ya se ha comentado anteriormente, la empresa G dispone de cuatro ámbitos de red con distinta infraestructura, cuyo punto en común son los Catalyst 6509 y los MX480 o, en otras palabras, la distribución y el núcleo.

Los equipos integrados en esta infraestructura serán en su mayor parte Cisco Catalyst 3750X y Juniper EX4200. Para dar red a los servidores se utilizan modelos Juniper EX4200-48T, que disponen de 48 puertos de cobre y se usan como conmutadores de N2, aunque también están capacitados para realizar operaciones de N3. El acceso de usuarios está compuesto por Catalyst 3750X-48P, ofreciendo así PoE, una tecnología imprescindible para dar alimentación a los teléfonos de los puestos de usuarios. Esta familia de Cisco también proporciona red al entorno de Internet, aunque no aportan PoE, ya que este entorno no lo necesita, por lo que usan Cat3750X-48T.

Los equipos que dan servicio a los usuarios están repartidos por los cuartos técnicos de las diferentes plantas de los edificios. Los enlaces hacia la distribución (o *uplinks)* se realizan mediante LACP de cobre a 2Gbps, excepto varios de ellos que utilizan fibra, por estar situados a más de 100 metros del CPD.

A continuación se expone la situación actual de la infraestructura a un nivel global, ya que, aunque se vayan a realizar mejoras en alguna parte del esquema, estos equipos no se verán directamente afectados en la integración.

Dividiremos el acceso en dos partes. El primer diagrama (Figura 28) muestra los accesos de los entornos de usuarios y servidores directamente conectados a los 6509 o distribución. El segundo diagrama (Figura 29) muestra los accesos de oficinas e Internet conectados directamente a los equipos de núcleo, por lo que en esta infraestructura no existiría capa de distribución.

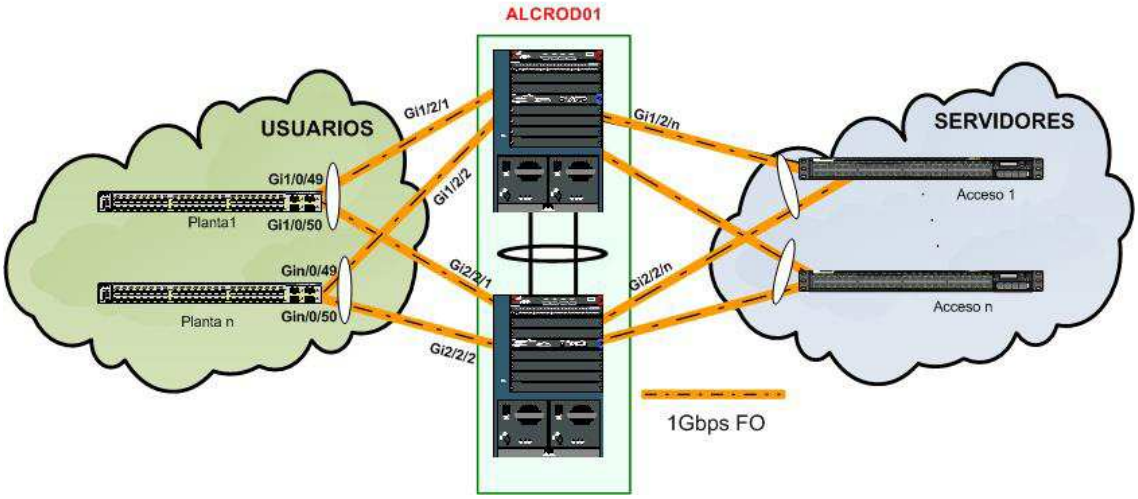


Figura 28: Interconexiones físicas de Servidores y Usuarios de la empresa G

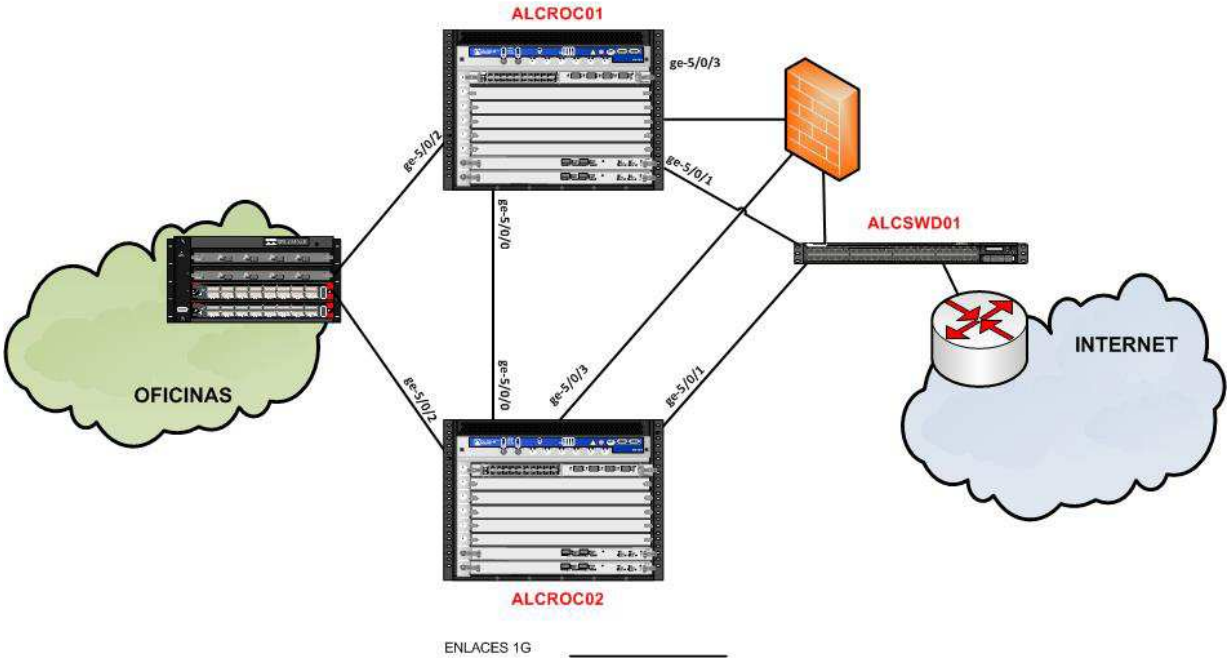


Figura 29: Interconexiones físicas de Internet y Oficinas de la empresa G

La infraestructura es simétrica en ambos CPDs, por lo que únicamente se muestra el diagrama de uno de ellos.

Tal y como se puede observar en los dos esquemas, los enlaces agregados están conectados de tal forma que cada uno va conectado a uno de los equipos de su capa superior. De esta manera, está ofreciendo doble redundancia:

- Redundancia a nivel de enlace: Si se cae uno de los enlaces, todo el tráfico irá por el otro enlace.
- Redundancia a nivel de equipo: Si se cae unos de los equipos de la distribución, todo el tráfico irá hacia el otro equipo levantado.

Esta forma de disponer los enlaces entre distintas capas se mantendrá a lo largo del proceso de integración de los CPDs.

Usuarios

El entorno de usuarios consta de equipos Cisco Catalyst 3750X de 48 puertos PoE de cobre independientes, instalados en los distintos cuartos técnicos de cada planta. Además, disponen de un módulo de cuatro puertos con opción a fibra para conectar dos de ellos a su distribución mediante agregación. Al igual que en la Empresa C, conectado a cada puerto de cobre de estos conmutadores, va un PC y un teléfono VoIP, utilizando la tecnología 802.1Q para dar servicio tanto a voz como a datos por el mismo enlace.

Servidores

El entorno de servidores a nivel de infraestructura, tanto física como lógica, es muy parecido al de los usuarios. Consta de conmutadores Juniper EX4200-48T repartidos por los distintos *racks* del CPD, cada uno con un agregado hacia la distribución, ya que también disponen de un módulo independiente de fibra, además de los 48 puertos de cobre.

Internet

Este entorno alberga toda aquella infraestructura que proporcione acceso de navegación a los puestos de usuario desde la LAN. Está compuesto por un conmutador Juniper EX4200 que interconecta el núcleo con el *firewall* de navegación y el enrutador del proveedor de Internet.

Oficinas

Este entorno comprende todo aquel tráfico entrante o saliente hacia la red de oficinas, siendo unas dos mil las que existen hoy en día. El Cisco Catalyst 6504 hace de interconexión entre la red MPLS de Oficinas y la LAN de la empresa G. Mediante dos enlaces de cobre de 1Gbps a cada MX, distribuirá el tráfico de las oficinas. Este entorno quedará intacto durante la integración, salvo la migración de enlaces de una tarjeta del núcleo a otra, como veremos más adelante en los apartados de la integración. Pero a nivel de configuración e infraestructura, se mantendrá igual.

3.2.2 Diseño lógico

Como ya hemos explicado anteriormente, tanto los equipos que se encuentran en los cuartos técnicos ofreciendo comunicación a los puestos de usuario, como los equipos que forman los distintos accesos, realizan funciones de nivel 2. Tienen un *gateway* por defecto

configurado apuntando al VSS, y éste será el que se encargue de encaminar el tráfico hacia el núcleo mediante el protocolo de encaminamiento OSPF.

A continuación se expondrá el listado de todo el direccionamiento/VLANes de cada uno de los entornos. Cabe destacar que todos los direccionamientos actuales de la empresa G son locales, es decir, que no se extienden a nivel 2 a través del enlace entre los CPDs.

	CPD LEGANÉS	VLAN ID	CPD ALCOBENDAS	VLAN ID
VLAN SERVIDORES_1	172.18.1.0/24	1000	172.18.4.0/24	1000
VLAN SERVIDORES_2	172.18.2.0/24	1001	172.18.5.0/24	1001
VLAN SERVIDORES_3	172.18.3.0/24	1002	172.18.6.0/24	1002
VLAN USUARIOS_1	172.20.1.0/24	2000	172.20.4.0/24	2000
VLAN USUARIOS_2	172.20.2.0/24	2001	172.20.5.0/24	2001
VLAN USUARIOS_3	172.20.3.0/24	2002	172.20.6.0/24	2002
VLAN INTERNET_1	172.30.1.0/24	3000	172.30.3.0/24	3000
VLAN OSPF_1	172.25.13.128/25	701	172.25.11.128/25	701
VLAN OSPF_2	172.25.14.128/25	702	172.25.12.128/25	702

Tabla 5: Direccionamiento/VLANes de la empresa G

Existen tres VLANes con direccionamiento de Clase C dedicadas a servidores en cada CPD. El nivel 3 de cada una de las VLANes lo tendrá la puerta de enlace, que en este caso es el Catalyst 6509, con un direccionamiento X.X.X.8/24. La misma casuística se da para los direccionamientos de usuarios. Para el entorno de Internet, es el FW el que llevará el N3 de estas VLANes, ya que es el que se encarga de encaminar, permitiendo o denegando el acceso al tráfico.

Las VLANes de OSPF son las que se utilizan para informar al núcleo de los direccionamientos de usuarios, servidores y oficinas.

La VLAN de Internet y Gestión se utilizan para dar conectividad de N2 entre el núcleo y los *firewall*.

Usuarios y Servidores

Todas las subredes o VLANes existentes en estos dos entornos son locales, es decir, que no se extienden a lo largo de los CPDs mediante N2. Para que ambos entornos entre los centros de datos se puedan comunicar, los equipos de núcleo necesitan informar a su pareja del otro CPD mediante rutas estáticas. La casuística que siguen los anuncios es la siguiente:

- MX1 de Alcobendas anuncia sus redes locales pares al MX1 de Leganés mediante rutas estáticas con peso 250.
- MX1 de Alcobendas anuncia sus redes locales impares al MX1 de Leganés mediante rutas estáticas con peso 200.
- MX2 de Alcobendas anuncia sus redes locales impares al MX2 de Leganés mediante rutas estáticas con peso 250.

- MX2 de Alcobendas anuncia sus redes locales pares al MX2 de Leganés mediante rutas estáticas con peso 200.

- MX1 de Leganés anuncia sus redes locales pares al MX1 de Alcobendas mediante rutas estáticas con peso 250.

- MX1 de Leganés anuncia sus redes locales impares al MX1 de Alcobendas mediante rutas estáticas con peso 200.

- MX2 de Leganés anuncia sus redes locales impares al MX2 de Alcobendas mediante rutas estáticas con peso 250.

- MX2 de Leganés anuncia sus redes locales pares al MX2 de Alcobendas mediante rutas estáticas con peso 200.

De esta manera, el tráfico cuyo destino es una red par siempre irá a través de los MX1 y el tráfico cuyo destino es una red impar siempre irá a través de los MX2.

Por otro lado, para que los equipos de núcleo sepan acceder a las subredes de usuarios y servidores, las distribuciones le anuncian estas redes mediante el protocolo de encaminamiento OSPF y, a su vez, estas reciben la ruta por defecto de cada MX.

Por tanto, el diagrama lógico queda de la siguiente manera:

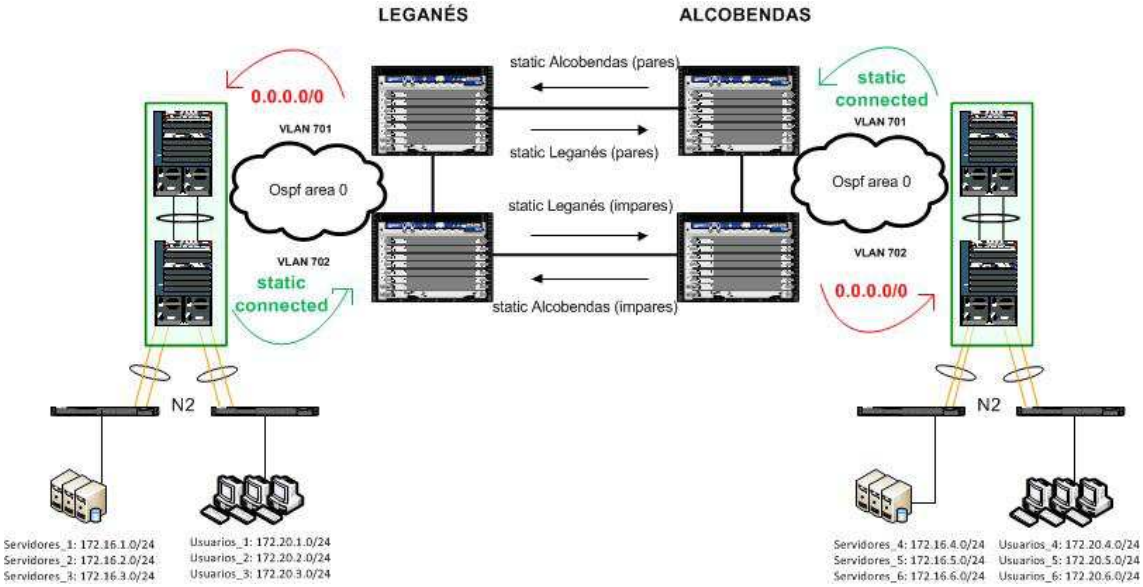


Figura 30: Interconexión lógica de Usuarios y Servidores de la empresa G

La distribución de usuarios y servidores anuncia al núcleo, por OSPF, todas las rutas que tenga como estáticas o como directamente conectadas.

Los equipos que hablan OSPF, lo hacen mediante interfaces VLAN configuradas como interfaces de nivel 3 y punto-a-punto. Aunque tengan la misma VLAN ID, no se solapan, al no estar extendidas a lo largo de los CPDs.

Se utiliza una VLAN por cada enlace de *uplink,* "VLAN 701" y "VLAN 702", para que en caso de caída del interfaz, la ruta desaparezca de la tabla de rutas sin necesidad de esperar al *timer* del protocolo. De esta forma mejoramos la convergencia, disminuyendo la probabilidad de pérdida de paquetes. Esta configuración en la red de servidores se mantendrá en la nueva integración.

En cuanto al direccionamiento, existe un DHCP conectado en la granja de servidores que proporciona direccionamiento dinámico a la red de usuarios. Los parámetros más relevantes que proporciona son:

- **Dirección IP**: Depende de la VLAN en la que esté configurado el puerto de usuario (PC + teléfono VoIP) y está comprendida entre la X.X.X.15 y la X.X.X.254. El resto de IPs se guardan para impresoras y para la puerta de enlace.
- **Máscara de subred**: Siempre tendrá el valor de 255.255.255.0 para todas las subredes de usuarios.
- **Puerta de enlace**: Corresponde al equipo de la distribución (Catalyst 6509) y este llevará la IP X.X.X.8 de cada una de las subredes.
- ***Domain Network Server*** **(DNS)**: Este servidor estará albergado en la granja y servirá a todas las redes de usuarios y servidores que lo necesiten.

Internet

La infraestructura de Internet es algo menos compleja ya que consiste en que todas las redes que no se aprenden por anuncios de OSPF, o bien porque son estáticos o bien porque estén directamente conectadas, se van a enviar al *firewall* de salida, que se encargará de denegar o permitir la conectividad hacia o desde Internet, además de realizar NAT para poder navegar hacia el exterior.

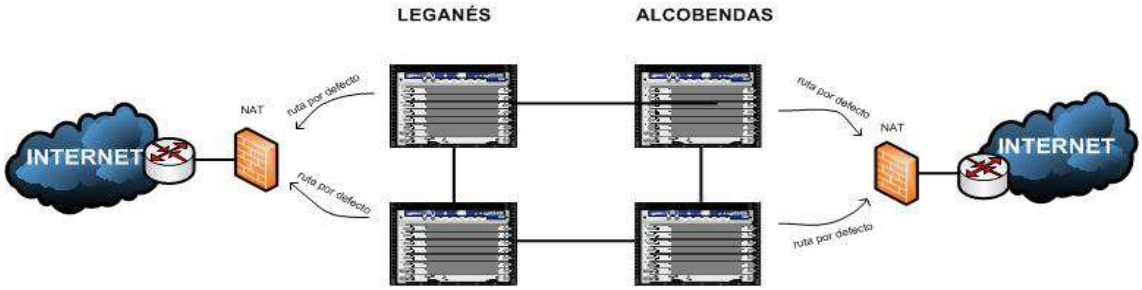


Figura 31: Interconexión lógica de Internet de la empresa G

Para este entorno no existe tráfico entre CPDs, ya que cada PC, teléfono o servidor navegará a través de su enrutador de proveedor local.

Un problema que existe en esta infraestructura es que si se cae uno de los dos enrutadores de acceso a Internet, los usuarios pertenecientes a ese CPD dejarán de poder navegar. Se contemplará una solución a este problema en el proceso de integración.

Oficinas

Existe un equipo Catalyst 6504 independiente que se encarga de hacer de distribución en el entorno de oficinas y encaminar el direccionamiento de estas hacia el núcleo. La red MPLS de oficinas contiene unos equipos de acceso que encaminan el tráfico a unos cifradores conectados a N2 de la distribución, que son los que se encargan de establecer los túneles para el tráfico cifrado de todas las oficinas externas de la empresa. Al existir dos redes MPLS – una en cada CPD – este entorno está diseñado de tal manera que las oficinas con direccionamiento

par entran por un CPD, mientras que las oficinas con direccionamiento impar entran por otro CPD. Es el acceso del proveedor, que no se contempla en este proyecto, quien filtra estos direccionamientos basándose en *route maps* y listas de acceso. Este diseño queda fuera del alcance de este proyecto, ya que su arquitectura se va a mantener exactamente igual después de la integración de ambas empresas.

Cada oficina tiene reservado un direccionamiento de clase C, por lo que cuando nos referimos a direccionamiento impar, nos referimos a aquellas oficinas en las que el segundo octeto es impar. La misma casuística ocurre para los direccionamientos pares.

4. PROBLEMAS Y MEJORAS PROPUESTAS

Una vez expuestas ambas arquitecturas de red, y con la finalidad de dar una solución altamente escalable y flexible, se estudiarán a continuación todos aquellos problemas identificados en ambas empresas, se intentará dar con una solución lo más adecuada posible a los requisitos del cliente. Además, se propondrán mejoras que supongan puntos fuertes para la fusión de las empresas.

4.1. EMPRESA C

Empezaremos analizando los problemas de la empresa C y proponiendo soluciones a los mismos.

4.1.1 Gestión y ACLs

Como ya se ha mencionado anteriormente, es imprescindible que los administradores de red sean capaces de llegar desde sus puestos de usuario a la gestión de sus equipos. Sin embargo, el problema recae en la total libertad de acceso a la gestión de los elementos de la red desde cualquier puesto de usuario que existe actualmente. Además, el tráfico de gestión y el de datos y multimedia comparten el mismo ancho de banda, por lo que estamos perdiendo disponibilidad de tráfico real de datos y multimedia en la red.

Otro problema existente es que, al compartir tráfico de gestión, datos y voz en lo mismos enlaces, cualquier avería de los conmutadores, VLANes, puertos físicos, etc. de los elementos de red, conllevará también una pérdida total de gestión de los mismos, y la única solución sería una conexión por consola a cada uno de los conmutadores localmente.

Para evitar estos problemas y obtener un buen control de los distintos elementos de red, se ha optado por utilizar listas de acceso que se encarguen de denegar cualquier conexión a los equipos, a excepción de los puestos de los técnicos que tengan permiso para acceder.

Un ejemplo de configuración de lista de acceso (ACL), siendo la IP 10.10.10.10 el puesto del administrador de red y 10.10.50.10 la IP de gestión de cualquier equipo, es:

access-list 10 permit tcp 10.10.10.10 0.0.0.0 10.10.50.0 0.0.0.255 eq telnet

access-list 10 permit tcp 10.10.10.10 0.0.0.0 10.10.50.0 0.0.0.255 eq ssh

access-list 10 deny ip any any

Para dar solución al problema de la gestión en banda, se propone configurar e instalar un nuevo entorno que dé servicio a la gestión de todos los elementos de red fuera de banda. De esta manera, los administradores podrán acceder a la misma a través del puerto Eth0 proporcionado en los Catalyst (o vme en los Juniper), para que no pierdan conexión si existiese algún fallo de configuración en los equipos, pérdida de conectividad con alguna subred, etc.

Ambas soluciones se utilizarán en la integración, por lo que estas configuraciones estarán en los tres CPDs.

4.1.2 Accesibilidad

En la actualidad, cualquier usuario tiene total libertad para poder acceder a cualquier otro PC, servidor o gestión de los equipos de red. Esto implica un inconveniente en la seguridad de una empresa y, por tanto, es algo que es imprescindible solventar.

Para resolver este problema, no sólo es necesario crear listas de acceso, sino considerar un replanteamiento de la infraestructura y dividirla en entornos de nivel 3 que, mediante encaminamiento dinámico o estático, permitan el acceso entre los distintos entornos. Esta solución se detallará más adelante cuando se hable de la solución a la integración entre ambas empresas.

4.1.3 Cisco StackWise

Actualmente, el edificio de la empresa C consta de 140 usuarios. Si tenemos en cuenta que cada conmutador tiene 48 puertos de cobre y considerando los puertos ocupados por los PCs, impresoras y enlaces entre distintos conmutadores, observaremos que solo quedan cuatro puertos libres en todo el edificio. Esto impide un crecimiento de usuarios en la empresa, lo que supone un gran problema de escalabilidad.

En el proceso de integración se instalará un conmutador Catalyst 3750X adicional por planta, formando una pila con el conmutador actual. De esta manera, se duplicará el número de puertos, obteniendo un índice de escalabilidad 1:2. La tecnología *StackWise* también proporcionará gran flexibilidad a la hora de ampliar la infraestructura, y dará doble redundancia a los usuarios, reduciendo a la mitad la caída de red de los puestos.

4.1.4 Redundancia a nivel de enlace

A simple vista, el escenario actual es claramente crítico en términos de redundancia. Nos podríamos encontrar un caso de caída de la distribución y, por tanto, en el que los usuarios dejarían de acceder a la red, estando completamente aislados de la misma.

En este proyecto se contemplará la instalación de dos nuevos equipos 6509 que conformarán la capa de distribución, obteniendo mayor disponibilidad de la misma. También obtendrán todas las ventajas que la tecnología VSS es capaz de ofrecer.

4.1.5 Otras

Para la nueva arquitectura de integración, la tecnología del ISP que utiliza la empresa actualmente, ADSL 2+, dejará de utilizarse, dando lugar a redes MPLS que permiten un mayor rendimiento de red.

En cuanto a la configuración de los puestos de usuario, se mejorará la seguridad de estos durante el proceso de integración, utilizando la tecnología *port security* y *storm control*. La seguridad de puerto se encargará de evitar que no más de dos MACs se conecten al puerto. Esto hará que no se conecten más de dos PCs o teléfonos a la vez, aumentando la seguridad de la red. La tecnología de *storm control* bloqueará el puerto en caso de que el tráfico *unicast*, *multicast* o *broadcast* supere el 50% del ancho de banda del puerto, evitando así tormentas

innecesarias que puedan producir saturación en la red. Esto se aplicará, de la misma manera, por toda la infraestructura integrada.

```
switchport port-security maximum 3

switchport port-security

storm-control broadcast level 50.00

storm-control multicast level 50.00

storm-control action shutdown
```

4.2. EMPRESA G

Estudiaremos ahora los problemas de la empresa G y qué opciones tenemos para solucionarlos.

4.2.1 Gestión

Al igual que en la empresa C, no existe un entorno de gestión como tal y, por tanto, constituye un punto crítico en cualquier parte de la arquitectura de red. Actualmente, para que los administradores puedan acceder a la red, se utilizan listas de acceso (ACLs) para denegar o permitir el acceso a la gestión en remoto de los equipos. En la integración se expondrá el diseño y configuración del entorno independiente de gestión.

4.2.2 Encaminamiento estático

El hecho de que una empresa con una arquitectura tan amplia no disponga de encaminamiento dinámico complica la gestión bajo demanda que existe e imposibilita un crecimiento dinámico de las necesidades de la empresa.

Es una arquitectura algo tediosa de mantener y de hacerla crecer tal y como se encuentra ahora por varios motivos, pero el más importante que cabe destacar es la disposición de VLANes/direccionamiento, que hacen de ellos entornos locales y poco flexibles a la hora de extenderse entre ambos CPDs. Es decir, cada vez que un equipo o usuario necesite alcanzar algún equipo o usuario del otro CPD, el núcleo tendrá que añadir rutas estáticas en cada uno de sus equipos, con diferentes pesos, para ofrecer la conectividad. Este será el principal problema que habrá que solventar en la solución del proyecto.

4.2.3 Ancho de banda

El ancho de banda que ofrecen actualmente los enlaces entre las tres capas es pequeño en comparación con el alto crecimiento de usuarios en la red, por lo que se pueden producir cuellos de botella y, por ende, problemas en la comunicación.

Un claro ejemplo es el uso de enlaces de 10Gbps entre los equipos Catalyst 6509 y los equipos que conforman el núcleo. En la actualidad utilizan un buen ancho de banda, ya que al estar configurado en LACP, llegan a proporcionar hasta 20Gbps por equipo; pero de nada sirve si las interconexiones entre ambos CPDs son enlaces de 1Gbps. Una forma de paliar este problema es aumentar los enlaces entre ambos CPDs, ofreciendo una interconexión de estrella, es decir, todos con todos.

4.2.4 Redundancia a nivel de tarjeta

Como se puede apreciar en las interconexiones entre los distintos componentes que conforman el núcleo y la distribución, todos los enlaces de los MXs parten de la misma tarjeta de red. Si ocurre algún problema en esta tarjeta (por ejemplo, un fallo en el *hardware*) y deja de dar conectividad, todos los enlaces que salen del MX caerán y, por tanto, dejará de haber redundancia a nivel de núcleo. Para ello, se instalarán cuatro tarjetas de red, una en cada MX, ofreciendo así una tercera redundancia (además de la de enlace y equipo), que es la redundancia de tarjeta de red.

4.2.5 Servidores *Blades*

La empresa G requiere instalar nuevas tarjetas *blades* una vez realizada la integración, que necesitan enlaces de 10G. Hay dos formas de dar conectividad a las cabinas mediante estos enlaces:

- **Ampliación de tarjetas:** Para dar conectividad a las cabinas, se instalaría una tarjeta de ocho puertos de 10Gbps (*WS-X6708-10G-3C*) en la distribución de los Catalyst 6509. Si se requiriesen más, se ampliaría con más tarjetas, ya que estos Catalysts dispondrían de hasta 5 ranuras (o *slots)* para conectar tarjetas. La desventaja es el alto coste de estas tarjetas que rondan los 30.000 euros.
- **Ampliación de conmutadores/módulos:** Otra alternativa más económica es disponer módulos especiales para poder utilizar en los equipos de acceso de Servidores (Juniper EX4200). Estos módulos constan de cuatro puertos configurables, en los que podríamos utilizar los cuatro puertos a 1G, o dos de ellos a 10G. De esta manera, por cada conmutador podríamos conectar una cabina de *blades* disponiendo así de redundancia.

4.2.6 Acceso a Internet

Como ya se comentó en el apartado 3.2.2, actualmente existe un problema en la red de Internet, ya que tal y como está diseñada la infraestructura. Si un enrutador de salida a Internet se cae, los usuarios de ese CPD dejarán de tener acceso a Internet.

La solución de MPLS y VPLS que se dará en los próximos apartados paliará este problema, ya que los enrutadores de ambos CPDs (más el que se añada en el CPD de la empresa C) serán capaces de hablar VRRP y así ofrecer redundancia a los usuarios; si se cae uno de ellos, otro podrá asumir su rol para dar acceso a Internet.

5. DISEÑO DE LA SOLUCIÓN FINAL

Teniendo en cuenta todos los puntos de fallo y de mejora que tiene cada empresa, se procede a explicar detalladamente la arquitectura de red final, una vez que las empresas se integren a nivel de comunicaciones.

A continuación se exponen los requisitos más importantes que exige el cliente a la hora de realizar la integración:

- Para paliar el problema de gestión fuera de banda de ambas empresas, se diseñará un entorno dedicado a la gestión. Esto quiere decir que tendrá su propia distribución y acceso, por lo que se instalarán equipos Juniper EX4200-24F, para la distribución, y EX4200-48T, para el acceso.

- Para mejorar el modo de acceso a las distintas arquitecturas de las empresas, se crearán entornos separados. Para ello se utilizarán las tecnologías MPLS VPN N3 (VRFs) y MPLS N2 (VPLS). Los entornos se clasificarán según el servicio ofrecido por las empresas:
  - SERVIDORES
  - USUARIOS
  - GESTIÓN
  - INTERNET
  - OFICINAS

Cada entorno dispondrá de su propia distribución y acceso, por lo que únicamente compartirán el núcleo.

- Para ofrecer una mayor escalabilidad, se utilizarán las tecnologías *Stackwise* (cuando se trate de equipos Cisco) o *Virtual Chassis* (cuando se trate de equipos Juniper) en todas las capas y entornos de ambas empresas.

- Se mejorará la redundancia utilizando, además de la tecnología de *stacking,* el protocolo LACP en todos aquellos enlaces acceso-distribución y distribución-núcleo donde se crea oportuno.

- Se aumentará el ancho de banda de las interconexiones entre CPDs para así evitar cuellos de botella actuales.

5.1. Nomenclatura

Durante todo el proceso de integración se nombrarán los equipos de acuerdo a un esquema acordado con el cliente.

La nomenclatura consensuada es la siguiente:

Nombre del equipo = ***[CPD]+[Función]+[Capa]+[Entorno]+[Nº de equipo]***

- ***CPD:*** Indica el CPD al que pertenece. Estos pueden ser:
  - Alcobendas = ***ALC***
  - Leganés = ***LEG***
  - Getafe = ***GET***
- **Función**: Indica qué función desempeña a nivel de Capa OSI:
  - N2 o *switch*= ***SW***
  - N3 o *router* = ***RO***
- **Capa**: Indica a qué capa de la arquitectura corresponde. Estas pueden ser:
  - Acceso = ***AC***
  - Distribución = ***D***
  - Núcleo/Core = ***C***
- **Entorno***:* Indica a qué entorno pertenece. Estos pueden ser:
  - Servidores = ***S***
  - Usuarios = ***U***
  - Gestión = ***G***
  - Internet = ***I***
  - Oficinas = ***O***
- **Nº de equipo:** Indica la numeración de equipos en caso de existir más de uno en cada núcleo, distribución o acceso.

Por ejemplo, un primer equipo situado en Leganés como equipo de acceso dando N3 en el entorno de servidores, se nombraría como **LEGROACS01.**

5.2. Configuración Física

5.2.1 Núcleo

El punto de unión entre las dos empresas será el núcleo de la red y en ambas se instalará la misma infraestructura. Para ello, la empresa globalmente dispondrá de 6 equipos Juniper MX480, dos en cada CPD. Los chasis MX480 disponen de 8 *slots* y pueden albergar hasta 6 tarjetas de línea (las otras dos restantes están reservadas para las supervisoras).

Para dar conectividad a cada una de las capas de distribución, se hará una ampliación de tarjetas, en cuyos puertos se configurará cada una de las interconexiones. Se propone, como ejemplo, uno de los tres CPDs:

- **ICX Núcleos**: la interconexión entre los MX del núcleo se hará mediante enlaces a 10Gbps.
- **ICX Núcleo – Distribución Usuarios:** Se conectarán mediante un enlace de 10Gbps desde cada MX al equipo de distribución.
- **ICX Núcleo – Distribución Servidores:** Se conectarán mediante dos enlaces de 10Gbps mediante LACP desde cada MX al equipo de distribución.
- **ICX Núcleo – Distribución Oficinas:** Se conectarán mediante dos enlaces de 1Gbps desde cada MX al equipo de distribución.
- **ICX Núcleo – Distribución Gestión:** Se conectarán mediante un enlace de 1Gbps desde cada MX al equipo de distribución (*firewall).*
- **ICX Núcleo – Distribución Internet:** Se conectarán mediante dos enlaces de 1G desde cada MX al equipo de distribución (*firewall).*

Al disponer sólo de una tarjeta de 4 puertos 10GbE, se necesita la ampliación de este tipo de puertos y, por tanto, una ampliación de las tarjetas en cada MX, dando como resultado lo siguiente:

Figura 32: Disposición de tarjetas del núcleo antes y después de la integración

Las tarjetas que se utilizarán serán las siguientes:

- ***Slot* 5 - DPCE-R-20GE-4XGE**: Contiene 20 puertos Gigabit Ethernet (1Gbps) y 4 puertos 10 Gigabit Ethernet.

Figura 33: Tarjeta DPCE-R-20GE-4XGE

- ***Slot* 4** - **DPC-R-4XGE-XFP:** Contiene 4 puertos 10 Gigabit Ethernet.

Figura 34: Tarjeta DPCE-R-4XGE-XFP

A continuación se muestra el resultado de ejecutar *show chassis hardware* en un MX por CLI (interfaz de comandos):

```
                                    Hardware inventory:
Item             Version  Part number  Description
Chassis                                 MX480 Midplane
Midplane         REV 05   710-017414   MX480 Midplane
FPM Board        REV 02   710-017254   Front Panel Display
PEM 0            Rev 01   740-022697   PS 1.2-1.7kW; 100-240V AC in
PEM 1            Rev 01   740-022697   PS 1.2-1.7kW; 100-240V AC in
PEM 2            Rev 01   740-022697   PS 1.2-1.7kW; 100-240V AC in
PEM 3            Rev 01   740-022697   PS 1.2-1.7kW; 100-240V AC in
Routing Engine 0 REV 09   740-013063   RE-S-2000
Routing Engine 1 REV 09   740-013063   RE-S-2000
CB 0             REV 03   710-021523   MX SCB
CB 1             REV 03   710-021523   MX SCB
FPC 4            REV 10   750-021566   DPCE 4x 10GE R
CPU            REV 03   710-022351   DPC PMB
PIC 0                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 1                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 2                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 3                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
FPC 5            REV 13   750-022765   DPCE 20x 1GE + 4x 10GE R
CPU            REV 03   710-022351   DPC PMB
PIC 0                     BUILTIN      10x 1GE(LAN)
Xcvr 0         REV 02   740-011613   SFP-SX
Xcvr 1         REV 02   740-011613   SFP-SX
Xcvr 2         REV 01   740-031851   SFP-SX
Xcvr 3         REV 02   740-011613   SFP-SX
Xcvr 4         REV 02   740-011613   SFP-SX
Xcvr 5         REV 01   740-038291   SFP-T
Xcvr 6         REV 02   740-011613   SFP-SX
Xcvr 7         REV 02   740-011613   SFP-SX
Xcvr 8         REV 01   740-038291   SFP-T
Xcvr 9         REV 01   740-031851   SFP-SX
PIC 1                     BUILTIN      10x 1GE(LAN)
Xcvr 0         REV 01   740-031851   SFP-SX
Xcvr 1         REV 01   740-031851   SFP-SX
Xcvr 2         REV 01   740-031851   SFP-SX
Xcvr 3         REV 01   740-031851   SFP-SX
Xcvr 4         REV 01   740-031851   SFP-SX
Xcvr 5         REV 01   740-031851   SFP-SX
Xcvr 6         REV 01   740-038291   SFP-T
Xcvr 7         REV 02   740-013111   SFP-T
Xcvr 9         REV 01   740-031851   SFP-SX
PIC 2                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 3                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 4                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
PIC 5                     BUILTIN      1x 10GE(LAN/WAN)
Xcvr 0         REV 03   740-014289   XFP-10G-SR
```

Una vez ampliadas las tarjetas, se instalarán los MX480 en el CPD de la empresa C, eliminando el enrutador que hace de núcleo actualmente, y se dará conectividad hacia el resto de MX mediante enlaces a 10Gbps, resultando una infraestructura de interconexión de núcleo de la siguiente manera:

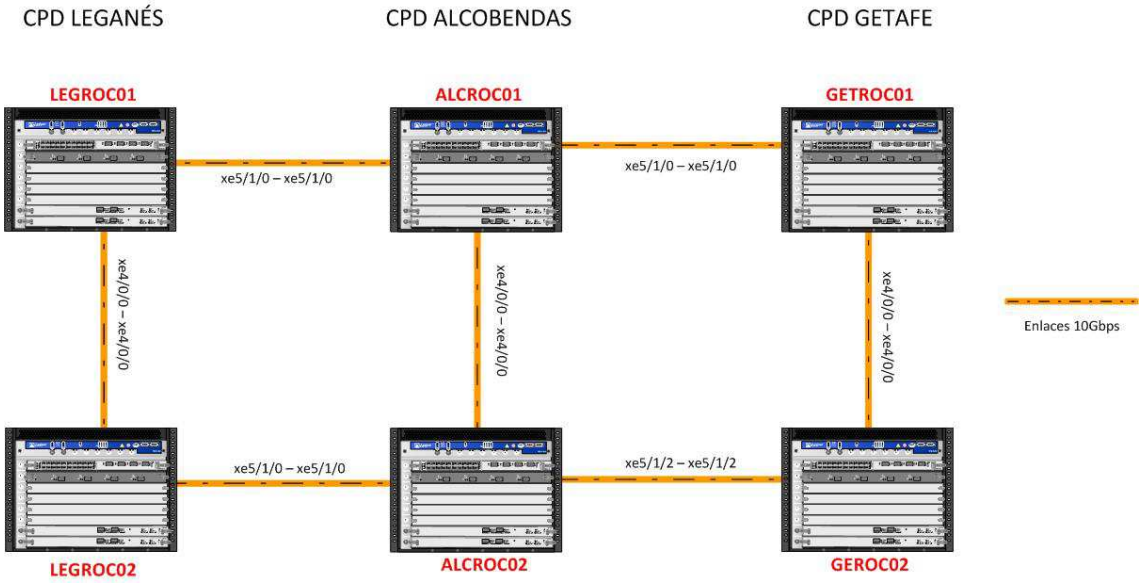


Figura 35: Interconexión final de los MX del núcleo

El motivo por el que se ha interconectado de esta manera tiene que ver con las distancias que separan a estos tres CPDs. Para aprovechar al máximo la fibra oscura, se ha decidido utilizar aquella que menos costes tenga. Para ello, se ha conectado Leganés con Getafe, que son los más cercanos.

Cabe mencionar que en cada CPD se dispone de equipos *multiplexadores DWDM* que son los que interconectan físicamente las fibras entre los CPDs. Los *DWDM* los gestiona un operador externo y, por tanto, deberán proporcionar en este proyecto el equipamiento necesario para su interconexión.

Desde cada uno de los enlaces a 10Gbps que interconectan los MX, los enlaces se distribuyen entre los dos *slots* o ranuras del chasis, consiguiendo así redundancia de tarjetas.

Durante la integración, los técnicos reconfigurarán todos los puertos para que queden como en el esquema de la Figura 35.

5.2.2 Distribuciones y Accesos

Como parte de los requerimientos del cliente, es de gran importancia para esta integración separar cada entorno, tanto física como lógicamente.

Para ello, cada entorno dispondrá de su propia capa de distribución y acceso, teniendo únicamente como punto en común el núcleo o, lo que es lo mismo, los Juniper MX480 de su correspondiente CPD.

A continuación se describirá la parte de interconexiones físicas de cada uno de los entornos por separado.

Servidores

Para dar servicio a la parte de servidores, la Empresa G aprovechará los Catalyst 6509 que ya tienen configurados en ***Virtual Switching System (VSS)***. El tráfico a usuarios lo proporcionarán otros equipos distintos que se detallarán más adelante.

Para mejorar tanto la redundancia como la escalabilidad, se instalarán, además, dos equipos Catalyst 6500 en la empresa C, formando un grupo VSS. La infraestructura y configuración será la misma que los 6500 instalados ya en la Empresa G, haciendo de ella una infraestructura simétrica en los tres CPDs.

Como se ha comentado anteriormente, un VSS permite que dos chasis 6500 actúen como uno solo. Para unir los dos chasis en un VSS se han utilizado dos enlaces agregados de fibra de 10Gb. Los puertos utilizados para el VSS son:

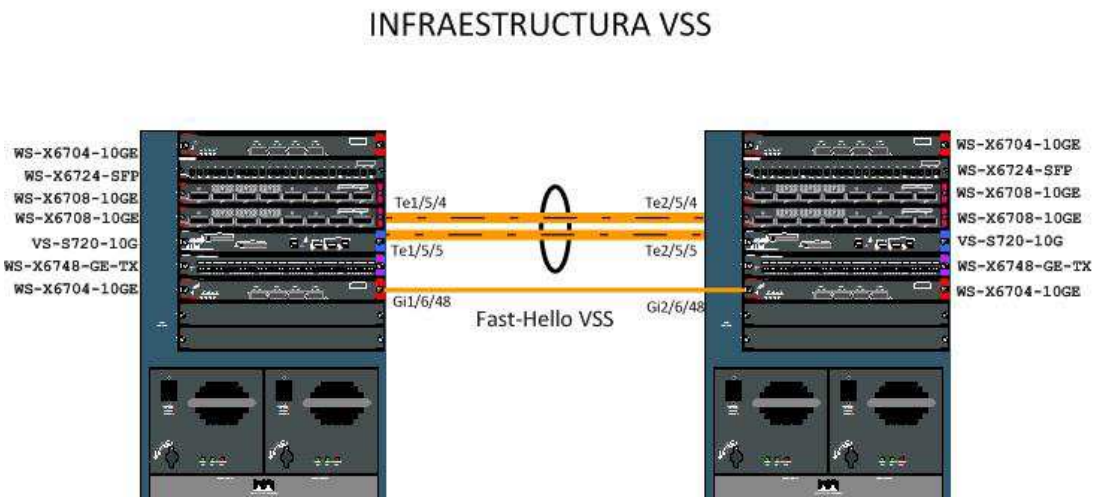
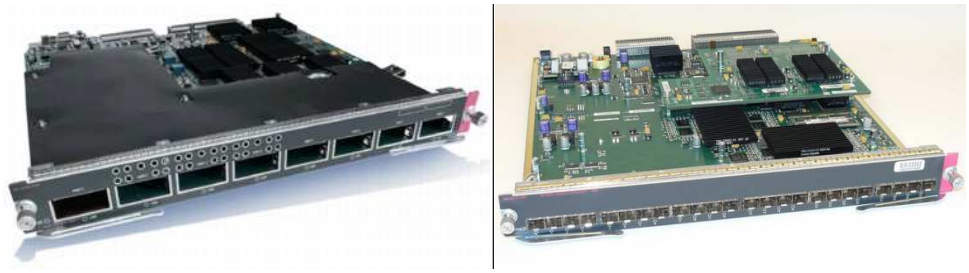


Figura 36: Disposición tarjetas y enlaces VSS – Distribución Servidores

Como medida de redundancia extra, se ha configurado otro enlace de respaldo para que los equipos se vean entre sí en todo momento, mediante el protocolo *Fast-hello*. Se trata de un enlace de 1Gbps. Los puertos utilizados son los mismos en los tres CPDs.

Para conocer un poco más en qué consiste cada Catalyst 6509, se añade un listado de las diferentes tarjetas que lo componen:

```
Servidores_1#sho module all
Mod Ports Card Type                                Model
--- ----- -------------------------------------- ------------------
  1     8  CEF720 8 port 10GE with DFC             WS-X6708-10GE
  2    24  CEF720 24 port 1000mb SFP               WS-X6724-SFP
  3     8  CEF720 8 port 10GE with DFC             WS-X6708-10GE
  4     5  Supervisor Engine 720 10GE (Backup)     VS-S720-10G
  5     5  Supervisor Engine 720 10GE (Active)     VS-S720-10G
  6    48  CEF720 48 port 10/100/1000mb Ethernet   WS-X6748-GE-TX
```



WS-X6708-10GE WS-X6724-SFP

VS-S720-10G WS-X6748-GE-TX

Figura 37: tarjetas a utilizar en la capa de distribución del entorno de servidores

- **WS-X6708-10GE:** Es una tarjeta de 8 puertos capaz de proporcionar 10 Gbps, soportando distancias de hasta 80 km sobre una misma fibra, y 15 m sobre cobre. Es en esta tarjeta donde se conectan los enlaces entre la distribución y el núcleo, ya que es un punto crítico de la arquitectura que necesita soportar mucha capacidad de tráfico.
- **WS-X6724-SFP:** Consiste en 24 puertos 1000BASE-SX para conectar SFPs de fibra a 1Gbps. Esta tarjeta se utiliza para conectar a la distribución cada uno de los accesos, formando LACP para aumentar la capacidad de tráfico a 2Gbps.
- **WS-X6748-GE-TX:** Esta tarjeta lleva 48 puertos de cobre, utilizados para conectar directamente, en caso de necesidad, servidores o equipos de monitorización.
- **VS-S720-10G:** Es la supervisora y la que se encarga de sincronizar todas las tarjetas y controlar todos los protocolos de red. Cada tarjeta únicamente trata la tabla de *forwarding* propia, por lo que diríamos que la supervisora es el cerebro del *chassis*.

A continuación se muestra la configuración de VSS en uno de los CPDs:

```
interface TenGigabitEthernet1/5/4
description VSS_Catalyst
no switchport
no ip address
mls qos trust cos
channel-group 1 mode on
end

interface TenGigabitEthernet1/5/5
description VSS_Catalyst
no switchport
no ip address
```

```
mls qos trust cos
channel-group 1 mode on
end

interface Port-channel1
description VSS
no switchport
no ip address
switch virtual link 1
mls qos trust cos
no mls qos channel-consistency
end

interface Port-channel2
description VSS
no switchport
no ip address
switch virtual link 2
mls qos trust cos
no mls qos channel-consistency
end


interface GigabitEthernet1/6/48
description fast-hello VSS
no switchport
no ip address
logging event link-status
dual-active fast-hello
end

interface GigabitEthernet2/6/48
description fast-hello VSS
no switchport
no ip address
logging event link-status
dual-active fast-hello
```

Cada VSS se ha conectado con los equipos del núcleo mediante dos enlaces agregados de 20Gbps, formando una capacidad total de 40Gb en la conexión de Leganés, 40Gb en la conexión de Alcobendas y 40Gbps en la conexión de Getafe. Los puertos utilizados para los enlaces se detallan en el punto siguiente.

LEGANÉS			ALCOBENDAS			GETAFE		
Agregado	**LEGRODS01**	**MXs (núcleo)**	**Agregado**	**Puerto VSS**	**MXs (núcleo)**	**Agregado**	**Puerto VSS**	**MXs (núcleo)**
1	Te1/1/4(Po71)	xe5/1/3 MX1	1	Te1/1/4(Po71)	xe5/1/3 MX1	1	Te1/1/4(Po71)	xe5/1/3 MX1
	Te2/1/6(Po71)	xe4/0/1 MX1		Te2/1/6(Po71)	xe4/0/1 MX1		Te2/1/6(Po71)	xe4/0/1 MX1
2	Te2/1/4(Po72)	xe5/1/3 MX2	2	Te2/1/4(Po72)	xe5/1/3 MX2	2	Te2/1/4(Po72)	xe5/1/3 MX2
	Te1/1/6(Po72)	xe4/0/1 MX2		Te1/1/6(Po72)	Xe4/0/1 MX2		Te1/1/6(Po72)	Xe4/0/1 MX2

Tabla 6: Puertos de interconexión entre el núcleo y la distribución de servidores

La interconexión entre el Núcleo y la distribución de Servidores queda de la siguiente manera:

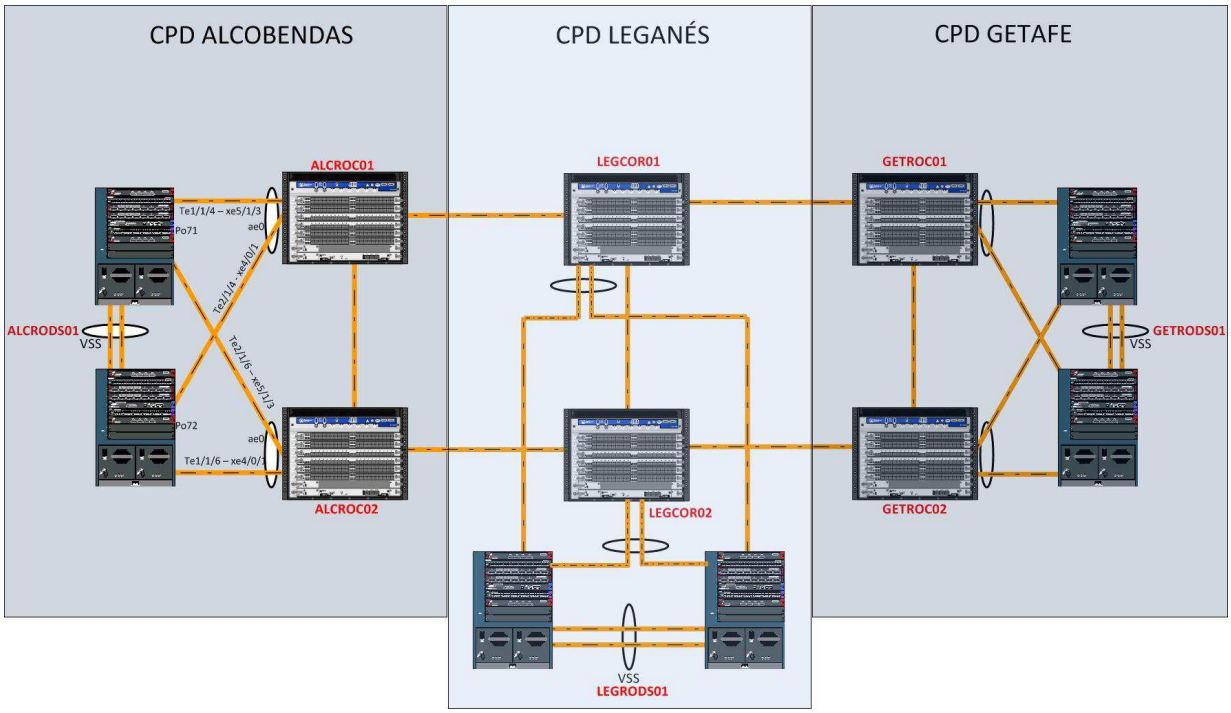


Figura 38: Esquema de interconexión entre el núcleo y la distribución de servidores

Como se observa en la figura 38, estas conexiones ofrecen redundancia a nivel de enlace utilizando LACP, redundancia a nivel de equipo (cada enlace de LACP conecta con un equipo diferente) y redundancia a nivel de tarjeta (cada enlace de LACP conecta con una tarjeta diferente).

Para dar conectividad directa a los servidores de la empresa C, bastará con reutilizar el que hay actualmente, el Cisco Catalyst 3750X-48P, y que de momento es suficiente para dar conectividad a los servidores que hay actualmente. Además de éste, se conectará otro Cisco 3750X-48T (más económico que el conmutador de 48 puertos *Power over Ethernet* (PoE), formando *stack* con el primero, para dar redundancia, tanto a nivel de enlace como de *chassis*, conectándolo con LACP a la distribución.

Figura 39: Catalyst 3750X-48P. Recuperado de
[http://www.cisco.com/c/en/us/support/switches/catalyst-3750x-48p-s-switch/model.html]

La capa de acceso en los CPDs de Alcobendas y Leganés estará formada por diferentes *chasis virtuales* de equipos Juniper EX4200-48T ubicados en diferentes *racks* del CPD. Estos equipos disponen de 48 puertos de cobre (sin *PoE)* dedicados exclusivamente a conectar servidores.

Figura 40: Juniper EX4200-48T.
[http://www.juniper.net/us/en/company/press-center/images/image-library/ex4200-48t/]

Además, estos EX4200 contienen otro módulo de cuatro puertos que se usará para conectar, mediante fibra óptica, estos equipos con la distribución de servidores mediante LACP. Este módulo se puede configurar para que los cuatro puertos funcionen a 1Gbps, o bien que dos de ellos funcionen a 10Gbps. En nuestro caso los configuraremos a 1Gbps contra la distribución o *VSS.*

El *chasis virtual* se configurará mediante cables especiales (*stack cables*), cuyos puertos (*stack ports)* se encuentran por detrás de estos conmutadores.

A continuación se expone la distribución y conectividad de equipos:

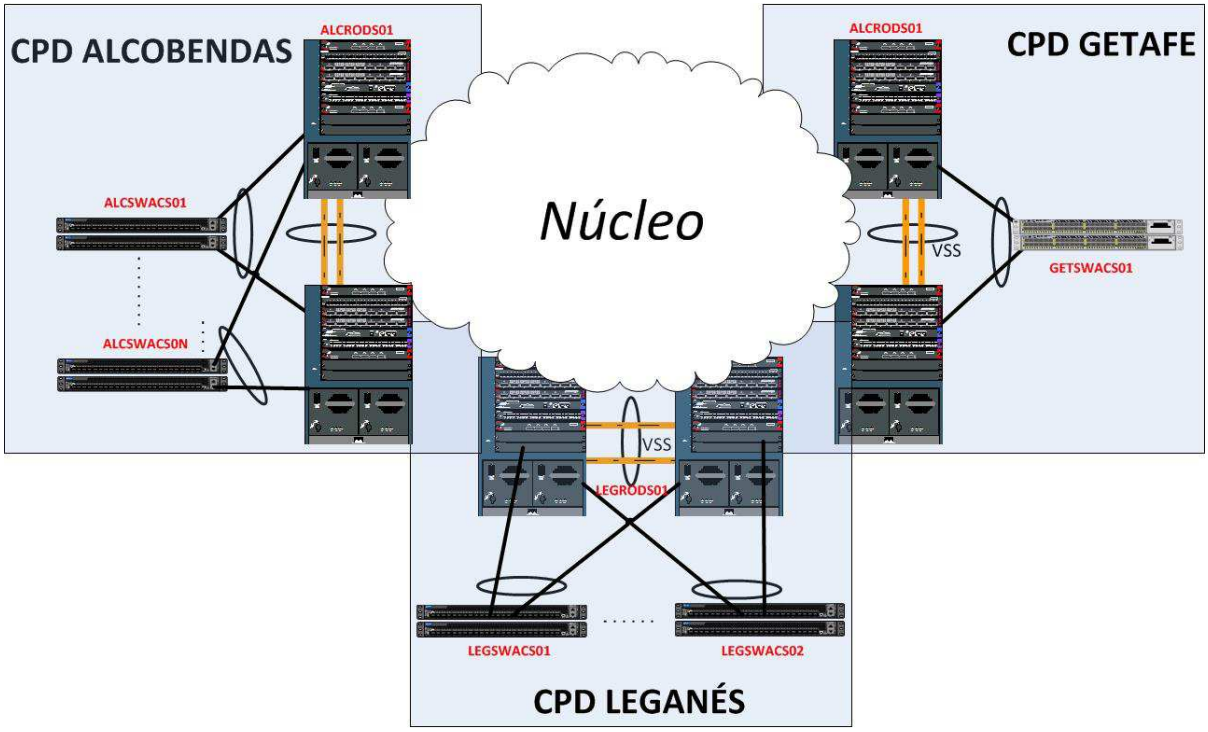


Figura 41: Esquema de interconexión entre la distribución y el acceso de servidores

LEGANÉS			ALCOBENDAS			GETAFE		
Agregado	**LEGRODS01**	**Accesos**	**Agregado**	**ALCRODS01**	**Accesos**	**Agregado**	**GETRODS01**	**Accesos**
1	Gi1/2/1	ge-0/1/0 LEGSWACS01	1	Gi1/2/1	ge-0/1/0 ALCSWACS01	1	Gi1/2/1	ge-0/1/0 GETSWACS01
	Gi2/1/1	ge-1/1/0 LEGSWACS01		Gi2/1/1	ge-1/1/0 ALCSWACS01		Gi2/1/1	ge-1/1/0 GETSWACS01
N	Gi1/2/N	ge-0/1/0 LEGSWACS0N	N	Gi1/2/N	ge-0/1/0 ALCSWACS0N	N	Gi1/2/N	ge-0/1/0 GETSWACS0N
	Gi2/1/N	ge-1/1/0 LEGSWACS0N		Gi2/1/N	ge-1/1/0 ALCSWACS0N		Gi2/1/N	ge-1/1/0 GETSWACS0N

Tabla 7: Puertos de interconexión entre la distribución y el acceso de servidores

Usuarios

A la distribución de usuarios se conectarán todos aquellos elementos de red que den conectividad únicamente a los puestos de usuario y/o teléfonos e impresoras. También se conectarán equipos de laboratorio o máquinas virtuales, si el cliente lo requiere.

La capa de distribución estará formada por cuatro equipos Juniper EX4200-24F en cada CPD configurados con la tecnología anteriormente descrita y llamada *Chasis Virtual*. Estos equipos disponen de 24 puertos de fibra para conectar los equipos de acceso y los equipos del núcleo, por lo que se utilizarán fibras en todas estas interconexiones.

Figura 42: Juniper EX4200-24F. Recuperado de www.juniper.net

Cada puerto de estos conmutadores consiste en un *slot* en el que se inserta un SFP-SX para dar la conectividad en fibra de hasta 1Gbps (las velocidades posibles son 10mbps, 100mbps o 1Gbps).

Además, se compone de otro módulo de dos puertos, que se usarán para formar el *chasis virtual* en fibra a 10Gbps. Esta configuración por fibra es mejor que la descrita en el apartado anterior, ya que el *throughput* es bastante mayor.

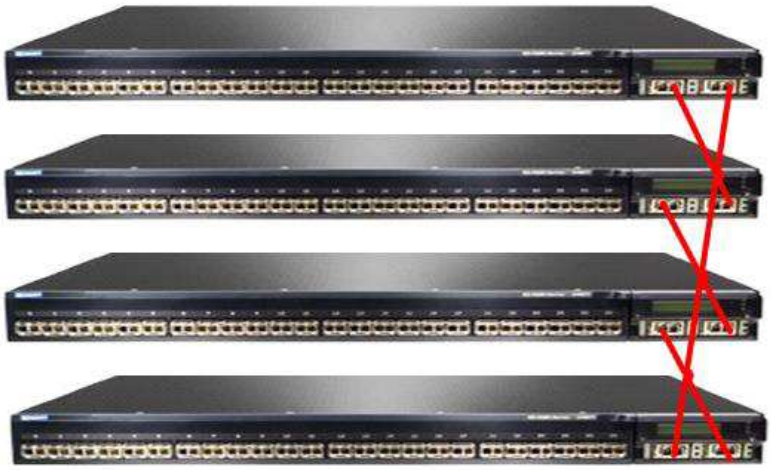


Figura 43: Chasis Virtual de modelos Juniper EX4200-24F.
[http://www.juniper.net/us/en/company/press-center/images/image-library/ex4200-24f/]

La Figura 43 muestra la disposición de los cables de fibra para formar el *Chasis Virtual*. Cada par de equipos estará ubicado físicamente en *racks* o armarios diferentes dentro de los CPDs, para dar redundancia a nivel de alimentación. De esta manera, si existiese algún microcorte o fallo eléctrico en uno de los *racks*, seguiría habiendo disponibilidad en el otro par de equipos, siempre que el fallo eléctrico no le hubiese afectado. Esta forma de disposición de los equipos en diferentes *racks* se mantendrá en el resto de equipamiento durante el proceso de integración.

Es importante mencionar que estos equipos disponen de doble fuente de alimentación con el fin de dar redundancia, siempre y cuando estén conectados, cada uno, a distintas fases. Para ser más concretos: todos los equipos de la electrónica de red dispondrán de doble fuente de alimentación.

Figura 44: Ejemplo de doble fuente de alimentación en Juniper EX4200-24F. Recuperado de www.juniper.net

A continuación se expone la configuración del *chasis virtual* mediante los enlaces de fibra que se formarán a través del primer puerto 10Gbps de cada conmutador:

```
set chassis fpc 0 pic 1 sfpplus pic-mode 10g
set chassis fpc 1 pic 1 sfpplus pic-mode 10g
set chassis fpc 2 pic 1 sfpplus pic-mode 10g
set chassis fpc 3 pic 1 sfpplus pic-mode 10g

set virtual-chassis preprovisioned
set virtual-chassis member 0 role routing-engine
set virtual-chassis member 0 serial-number BR0204921
set virtual-chassis member 1 role routing-engine
set virtual-chassis member 1 serial-number BR0220353
set virtual-chassis member 2 serial-number BR0220327
set virtual-chassis member 3 serial-number BR0221566
```

El siguiente esquema ofrece el resultado de las interconexiones en el entorno de Usuarios:

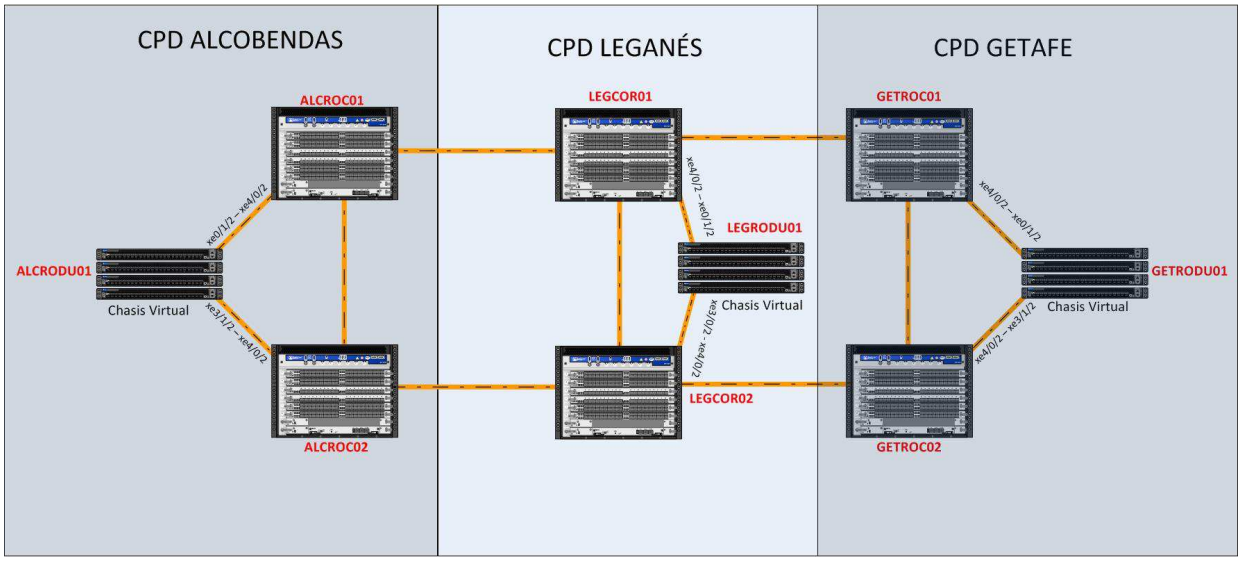


Figura 45: Esquema de interconexión entre la distribución y el núcleo de usuarios

Aunque en este entorno no existen agregados entre la distribución y el núcleo, existen dos enlaces a 10Gbps aportando suficiente ancho de banda para dar conectividad a todos los usuarios.

LEGANÉS		ALCOBENDAS		GETAFE	
LEGRODU01	**MXs (núcleo)**	**ALCRODU01**	**MXs (núcleo)**	**GETRODU01**	**MXs (núcleo)**
xe-0/1/2	xe4/0/2 MX1	xe-0/1/2	xe4/0/2 MX1	xe-0/1/2	xe4/0/2 MX1
xe-3/1/2	xe4/0/2 MX2	xe-3/1/2	xe4/0/2 MX2	xe-3/1/2	xe4/0/2 MX2

Tabla 8: Puertos de interconexión entre la distribución y el núcleo de usuarios

Para dar conectividad directa a los usuarios de la empresa C se reutilizarán los conmutadores Cisco Catalyst 3750X-48P que hay actualmente, ya que el número de usuarios no va a aumentar de momento.

La capa de acceso en los CPDs de Alcobendas y Leganés estarán formadas por diferentes pilas S*tackWise* de equipos Cisco Catalyst 3750X-48P ubicados en diferentes cuartos técnicos de las plantas de los edificios. Estos equipos disponen de 48 puertos de cobre (con *PoE)* dedicados exclusivamente para conectar usuarios, teléfonos e impresoras.

Los enlaces a la distribución (*Chasis Virtual* de cuatro equipos Juniper EX4200), serán enlaces dobles de 1Gbps (2x1Gbps) formando LACP.

A continuación se expone la distribución y conectividad de equipos:

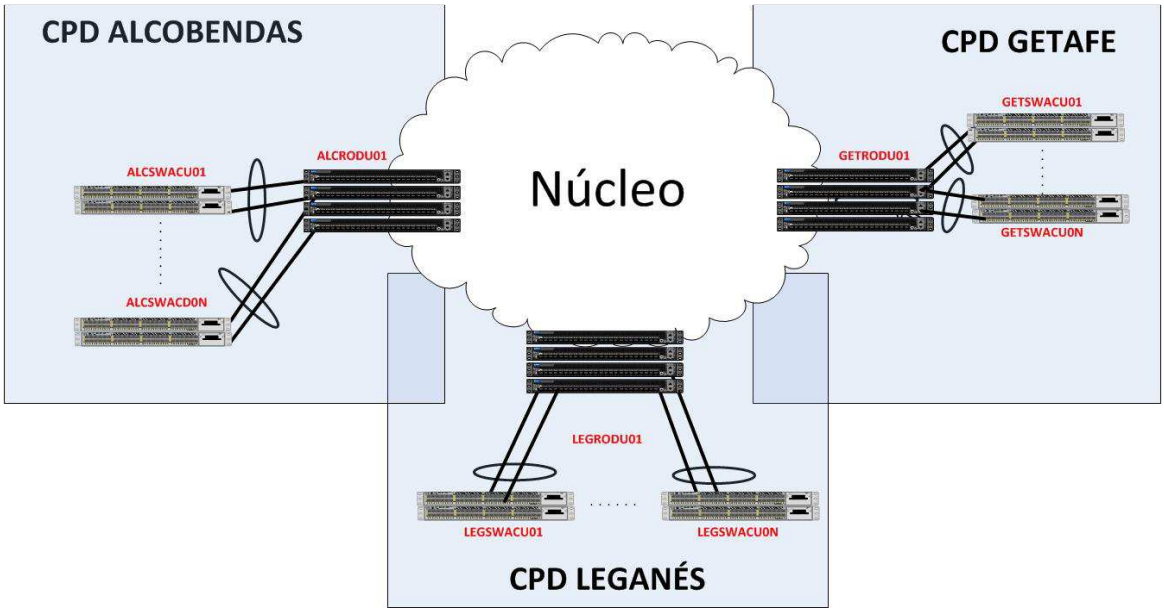


Figura 46: Esquema de interconexión entre la distribución y el acceso de usuarios

LEGANÉS			ALCOBENDAS			GETAFE		
Agregado	**LEGRODU01**	**Accesos**	**Agregado**	**ALCRODU01**	**Accesos**	**Agregado**	**GETRODU01**	**Accesos**
1	ge-0/0/1	Gi1/1/1 LEGSWACU01	1	ge-0/0/1	Gi1/1/1 ALCSWACU01	1	ge-0/0/1	Gi1/1/1 GETSWACU01
	ge-1/0/1	Gi1/1/2 LEGSWACU01		ge-1/0/1	Gi1/1/2 ALCSWACU01		ge-1/0/1	Gi1/1/2 GETSWACU01
N	ge-0/0/N	Gi1/1/1 LEGSWACU0N	N	ge-0/0/N	Gi1/1/1 ALCSWACU0N	N	ge-0/0/N	Gi1/1/1 GETSWACU0N
	ge-1/0/N	Gi1/1/2 LEGSWACU0N		ge-1/0/N	Gi1/1/2 ALCSWACU0N		ge-1/0/N	Gi1/1/2 GETSWACU0N

Tabla 9: Puertos de interconexión entre la distribución y el acceso de usuarios

Gestión

El entorno de gestión será un entorno nuevo que se instalará y configurará durante el proceso de integración en los tres CPDs con la finalidad de separar todo el tráfico de gestión a través de medios físicos y lógicos.

Este entorno tendrá su propia distribución y accesos, cuyos elementos de red gestionarán el resto de equipos de servidores, usuarios, etc. a través de los puertos fuera de banda.

El N3 lo realizará un *firewall* Fortigate 1240B instalado en cada uno de los 3 CPDs, que se encargará de denegar o permitir el acceso desde otras redes a las redes de gestión o viceversa. El *firewall* utilizado en la empresa C se usará para dar conectividad a este entorno de gestión.

Para no saturar todos los puertos del *firewall* y conectar todos los accesos a éste, se instalará un *chasis virtual* de EX4200-48T intermedio haciendo de distribución de N2, quedando de la siguiente manera:

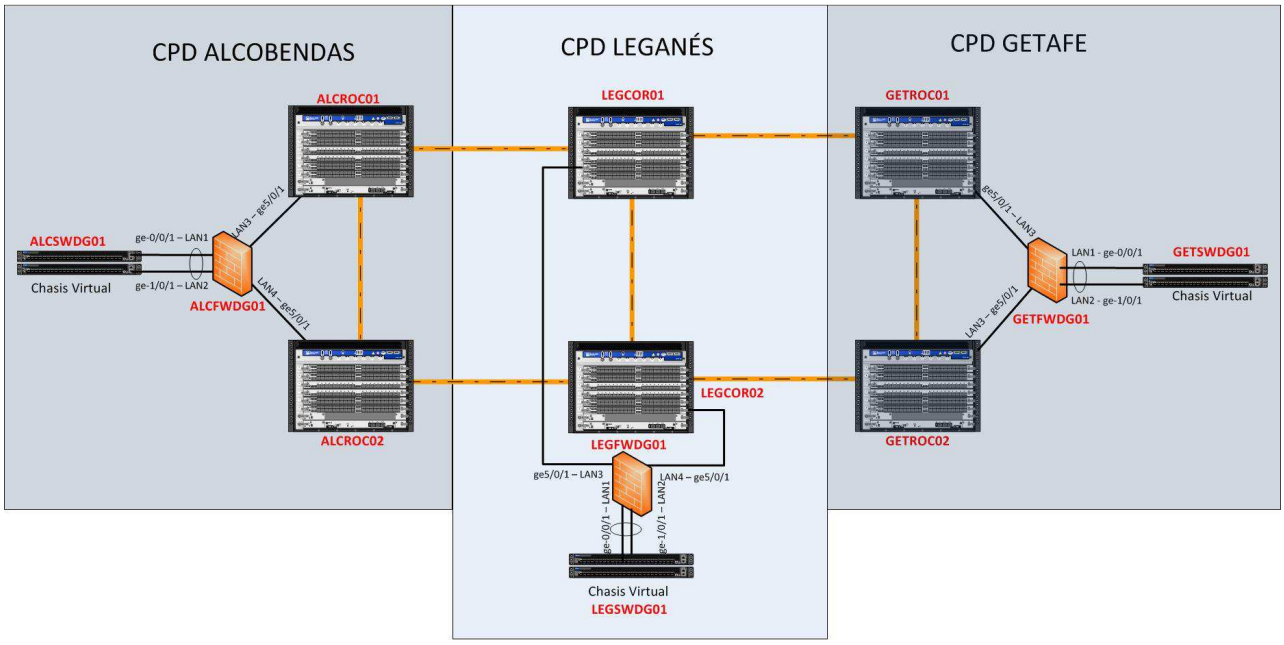


Figura 47: Esquema de interconexión entre la distribución y el núcleo de gestión

Todos los enlaces que conforman este entorno son enlaces de 1Gbps, ya que la gestión no necesita mucho ancho de banda debido al poco tráfico que cursa en comparación con otros entornos, por lo que aprovecharemos puertos de 1Gbps en los MX de la capa núcleo.

LEGANÉS			ALCOBENDAS			GETAFE		
LEGFWDG01	**LEGSWDG01**	**LEGRCO01**	**ALCFWDG01**	**ALCSWDG01**	**ALCRCO01**	**GETFWDG01**	**GETSWDG01**	**GETRCO01**
LAN1	ge-0/0/1		LAN1	ge-0/0/1		LAN1	ge-0/0/1	
LAN2	ge-1/0/1		LAN2	ge-1/0/1		LAN2	ge-1/0/1	
LAN3		ge-5/0/1	LAN3		ge-5/0/1	LAN3		ge-5/0/1
LAN4		ge-5/0/1	LAN4		ge-5/0/1	LAN4		ge-5/0/1

Tabla 10: Puertos de interconexión entre la distribución y el núcleo de gestión

El equipo intermedio lo formarán dos equipos Juniper EX4200-24F (modelo descrito en el punto 5.1.2) configurados en *chasis virtual* y formando agregación o LACP con el *firewall*. El motivo de este diseño se aclarará en el apartado de la configuración lógica del entorno.

La capa de acceso de la red de gestión en los tres CPDs estará formada por conmutadores independientes o formando pila distribuidos por los CPDs, ofreciendo gestión a los equipos del resto de entornos, tanto a equipos de acceso, como de distribución, como al núcleo. Serán equipos EX4200-48T.

También servirán para dar gestión a cualquier elemento de red ubicado en el CPD que necesite interfaces de gestión. Para gestionarlos, se conectará uno de los 48 puertos de estos conmutadores con el puerto *virtual management Ethernet (vme0* de Juniper) o con el puerto *ethernet (eth0* de Cisco). Estos puertos se consideran de gestión fuera de banda y se encuentran localizados en la parte posterior del conmutador. Estos puertos soportan 1Gbps de velocidad mediante enlaces de cobre.

Figura 48: Puertos fuera de banda en modelos Cisco. Recuperado de www.cisco.com

Figura 49: Puertos fuera de banda en modelos Juniper. Recuperado de www.juniper.net

Los enlaces a la distribución (*Chasis Virtual* de cuatro equipos Juniper EX4200-48T), serán enlaces dobles de 1Gbps (2x1Gbps) formando LACP.

Es importante mencionar que la pérdida de gestión de uno de estos equipos no supone una degradación del servicio, únicamente nos quedaríamos sin poder gestionar el equipo, pero seguiría dando servicio a los usuarios a través de los puertos de cobre del módulo de la parte delantera.

La distribución de estos equipos de acceso a lo largo de los CPDs irá en función del resto de equipos. Normalmente por cada 10 ó 12 equipos, independientemente del entorno que sea, se instalará un equipo de gestión para gestionarlos.

También se colocará un equipo de gestión en cada uno de los armarios de las diferentes plantas para gestionar los equipos de planta que dan servicio a los usuarios.

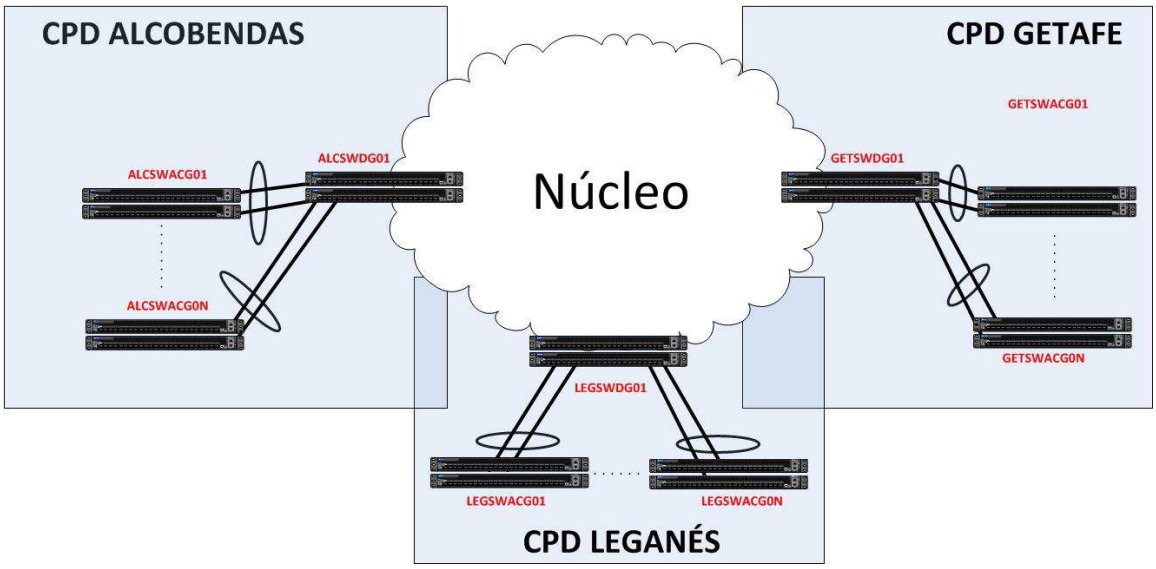


Figura 50: Esquema de interconexión entre la distribución y el acceso de gestión

LEGANÉS			ALCOBENDAS			GETAFE		
Agregado	LEGSWDG01	Accesos	Agregado	ALCSWDG01	Accesos	Agregado	GETSWDG01	Accesos
1	ge-0/0/1	ge-0/1/0 LEGSWACU01	1	ge-0/0/1	ge-0/1/0 ALCSWACU01	1	ge-0/0/1	ge-0/1/0 GETSWACU01
	ge-1/0/1	ge-1/1/0 LEGSWACU01		ge-1/0/1	ge-1/1/0 ALCSWACU01		ge-1/0/1	ge-1/1/0 GETSWACU01
N	ge-0/0/N	ge-0/1/0 LEGSWACU0N	N	ge-0/0/N	ge-0/1/0 ALCSWACU0N	N	ge-0/0/N	ge-0/1/0 GETSWACU0N
	ge-1/0/N	ge-1/1/0 LEGSWACU0N		ge-1/0/N	ge-1/1/0 ALCSWACU0N		ge-1/0/N	ge-1/1/0 GETSWACU0N

Tabla 11: Puertos de interconexión entre la distribución y el acceso de gestión

Oficinas

El entorno de oficinas apenas sufrirá cambios durante el proceso de integración de las dos empresas. Todas las oficinas o sucursales se interconectan a través de los CPDs de Alcobendas y Leganés, y así quedará en el futuro. No se instalarán equipos de este entorno en el CPD de Getafe, ya que el dimensionado que existe hoy en día es suficientemente potente para dar un buen servicio a nivel de comunicaciones.

También se quedará intacta la forma en la que los CPDs se distribuyen el tráfico; las redes de oficinas impares (hablando en términos de IP) se aprenden con mayor prioridad en el CPD de Alcobendas, mientras que las redes de oficinas pares (hablando en términos de IP) se aprenden con mayor prioridad en el CPD de Leganés.

Al volverse un entorno separado a nivel lógico como los demás, su función sí que afectará en la configuración del N2 y N3 en el núcleo. Detallaremos esta última más adelante.

A continuación se expone el conexionado físico que tendrá después de la integración junto con la tabla de conexiones:

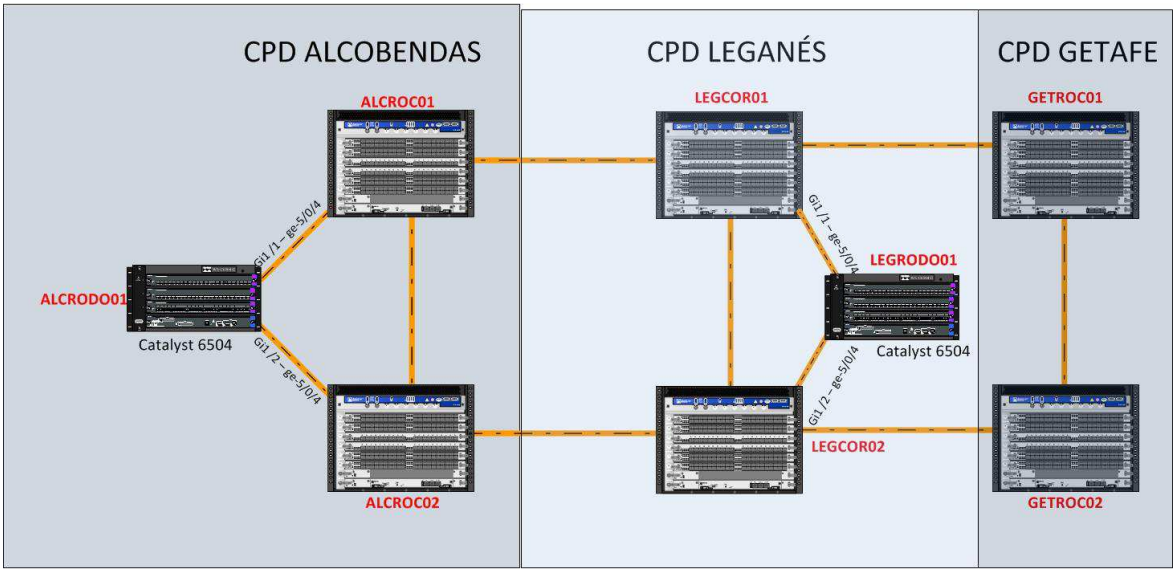


Figura 51: Esquema de interconexión entre la distribución y el núcleo de oficinas

LEGANÉS		ALCOBENDAS	
LEGRODO01	LEGROC01	ALCRODO01	ALCROC01
Gi1/1	ge5/0/4	Gi1/1	ge5/0/4
Gi1/2	ge5/0/4	Gi1/2	ge5/0/4

Tabla 12: Puertos de interconexión entre la distribución y el acceso de gestión

La infraestructura del acceso se quedará intacta durante la integración. Todo este entorno (acceso y distribución) lo gestiona un proveedor externo, ya que utiliza redes MPLS para dar conectividad a las oficinas, ajeno a la integración de este proyecto.

Internet

El modelo de infraestructura para este entorno se mantendrá muy parecido al que había anteriormente. Se instalará un *firewall* en cada uno de los CPDs junto a un conmutador de navegación para dar salida a Internet a través de un enrutador de proveedor. La función de este entorno es exclusivo para dar salida a Internet a los usuarios, por lo que 1Gbps de ancho de banda en cada CPD será suficiente.

Actualmente, cada CPD ofrece salida a Internet local. En el proceso de integración se diseñará de tal forma que habrá un CPD principal por el que cursará todo el tráfico hacia fuera y desde fuera, quedando los otros CPDs como respaldo en caso de caída del CPD principal.

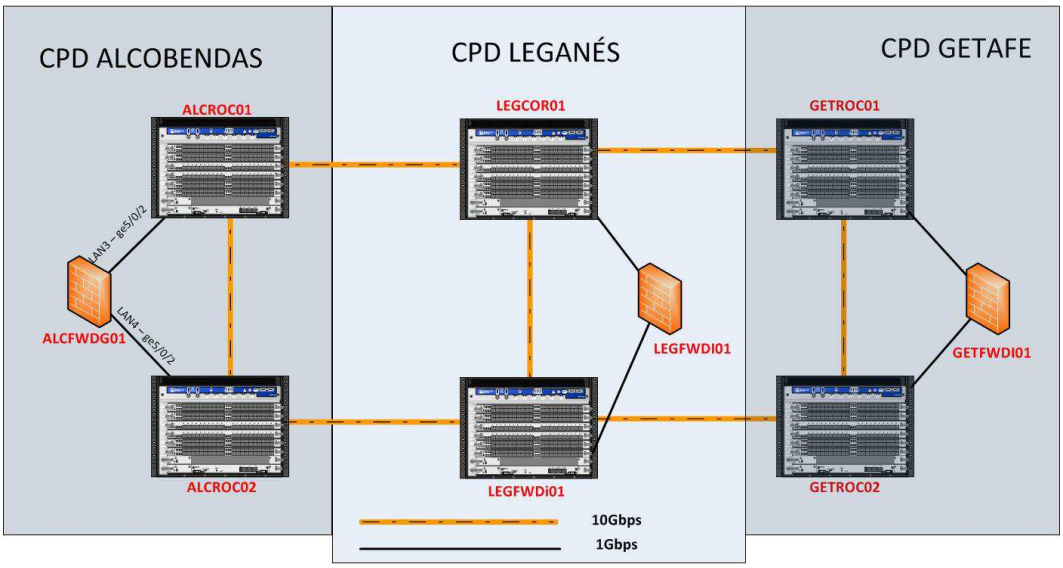


Figura 52: Esquema de interconexión entre la distribución y el núcleo de Internet

LEGANÉS		ALCOBENDAS		GETAFE	
LEGFWDI01	LEGCOR01	ALCFWDI01	ALCCOR01	GETFWDI01	GETCOR01
LAN3	ge-5/0/2	LAN3	ge-5/0/2	LAN3	ge-5/0/2
LAN4	ge-5/0/2	LAN4	ge-5/0/2	LAN4	ge-5/0/2

Tabla 13: Puertos de interconexión entre la distribución y el núcleo de Internet

Los conmutadores que harán de acceso de N2 y que conectan al *firewall* y al enrutador de salida a Internet serán dos equipos Juniper EX4200-48T formando *chasis virtual* y dando 1Gbps de conectividad en cada enlace.

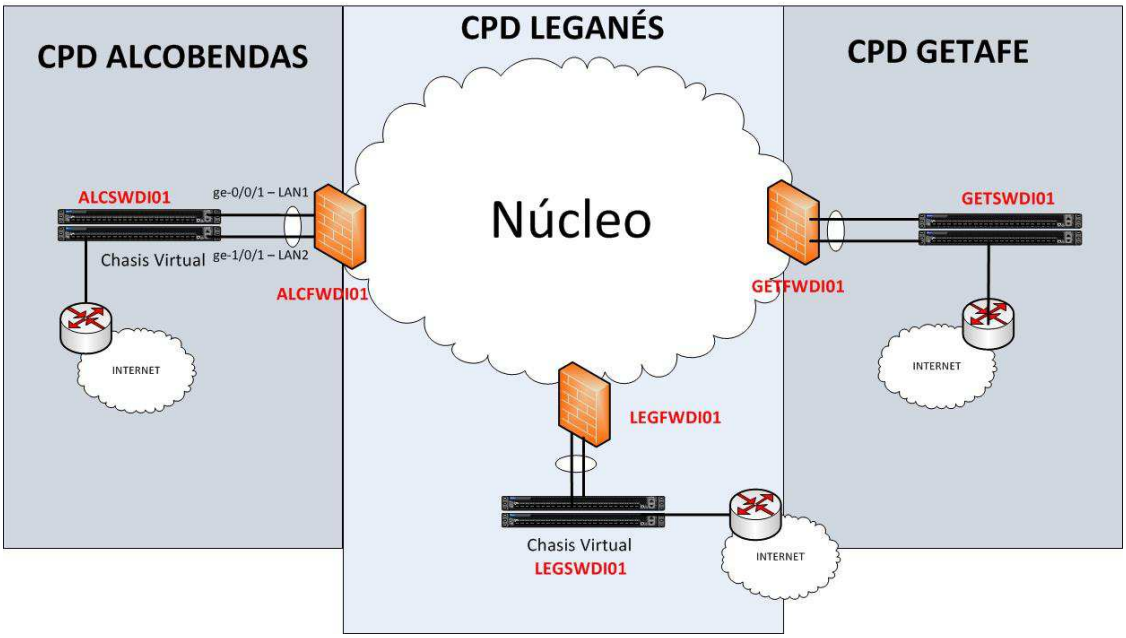


Figura 53: Esquema de interconexión entre la distribución y el acceso de Internet

LEGANÉS		ALCOBENDAS		GETAFE	
LEGFWDI01	**LEGSWDI01**	**ALCFWDI01**	**ALCSWDI01**	**GETFWDI01**	**GETSWDI01**
LAN1	ge-0/0/1	LAN1	ge-0/0/1	LAN1	ge-0/0/1
LAN2	ge-1/0/1	LAN2	ge-1/0/1	LAN2	ge-1/0/1

Tabla 14: Puertos de interconexión entre la distribución y el acceso de Internet

5.3. Configuración lógica

La topología lógica final de los CPDs integrados consistirá en una red compuesta por diferentes ámbitos en función del servicio que preste cada uno de ellos.

Antes de entrar en más detalle de configuraciones, tanto a nivel 2 como a nivel 3, hay que tener en cuenta los siguientes puntos acordados con el cliente:

La infraestructura final contendrá tres CPDs, cada uno con sus elementos físicos independientes, pero teniendo visibilidad todos con todos. Es decir, que la nueva empresa C tendrá que poder acceder a los servicios de la empresa G como si perteneciese a la misma LAN. Para ello, se ha decidido extender las subredes o VLANes a nivel 2 a lo largo de los tres CPDs, quedando de la siguiente manera:

- Los equipos Cisco 6500, EX4200 y *Firewall* pertenecientes a las distribuciones de los distintos entornos realizarán las funciones *Customer edge* –CE.
- Los equipos Juniper MX que forman el núcleo de toda la empresa realizarán las funciones de PE y P.
- Las tablas de rutas de la infraestructura MPLS formada por los 6 equipos Juniper MX se construyen mediante el protocolo iBGP.
- En las VPNs de nivel 2, la conmutación es responsabilidad de la capa de distribución (Cat6500, EX4200, FW), mientras que en las VPNs de nivel 3 es el núcleo (MX480) el que se encarga del encaminamiento.
- Existirá una instancia VPLS por cada VLAN extendida entre los tres CPDs, cuyo CE será la capa de distribución a la que pertenezca esa VLAN.

Por otro lado, se ha diseñado cada uno de los entornos por separado, teniendo en cuenta los siguientes requisitos:

- Las redes de Servidores deben extenderse a lo largo de los tres CPDs a N2, estando la ruta de todas las subredes, por defecto, en el CPD de Leganés.
- Las redes de Usuarios serán redes locales, es decir, que no se extenderán a N2, pero sí se extenderán por encaminamiento dinámico de N3 a lo largo de la interconexión del núcleo, ya que el resto de ámbitos pueden necesitar acceso a estas redes, o viceversa. Por tanto, la puerta de enlace de cada VLAN necesitará estar en su CPD correspondiente.
- Las redes de Internet y Gestión las gestionará el *firewall* propio de cada entorno y estarán extendidas a N2 a lo largo de los CPDs. El núcleo aprenderá estas redes mediante rutas estáticas, por lo que protocolos dinámicos de encaminamiento, como OSPF o BGP, no se utilizarán en estos ámbitos.
- La red de Oficinas se quedará intacta, por lo que no se instalará ningún dispositivo nuevo en la empresa C. Sus redes sí se deberán propagar a lo largo de los tres CPDs para dar conectividad total a las oficinas.

En base a estos requisitos previos, se explicará con detalle la solución a la integración de ambas empresas.

5.3.1 Direccionamiento del núcleo

Para las *interfaces* de *loopback* de los equipos del núcleo y las *interfaces* de conexión entre equipos, se dispone del rango de direccionamiento 172.25.10.0/24. Este rango se divide en las siguientes subredes a asignar en cada conexión:

RANGO	USO
172.25.10.0/30	Conexión Leganés1 – Alcobendas1
172.25.10.4/30	Conexión Alcobendas1 – Alcobendas2
172.25.10.8/30	Conexión Leganés2 – Alcobendas2
172.25.10.12/30	Conexión Leganés2 – Leganés1
172.25.10.16/30	Conexión Leganes1 - Getafe1
172.25.10.20/30	Conexión Getafe1 - Getafe2
172.25.10.24/30	Conexión Leganes2 - Getafe2
172.25.10.64/26	Reservado Futuro
172.25.10.128/26	Reservado Futuro
172.25.10.192/27	Reservado Futuro
172.25.10.224/28	Reservado Futuro
172.25.10.240/28	Red Loopback para iBGP
172.25.10.241/32	Loopback Leganés1
172.25.10.242/32	Loopback Leganés2
172.25.10.243/32	Loopback Alcobendas1
172.25.10.244/32	Loopback Alcobendas2
172.25.10.245/32	Loopback Getafe1
172.25.10.246/32	Loopback Getafe2
172.25.10.247 a 255/28	Reservado Loopback Núcleo

Tabla 15: Direccionamiento de las interfaces *loopback* del núcleo

5.3.2 Diseño MPLS VPN N3 y VPLS

En este apartado se definirán las configuraciones, tanto a N3 como a N2, en la infraestructura integrada.

A continuación se expone una tabla identificando las configuraciones a realizar en cada uno de los entornos:

Ámbito	VPLS	VPN3
Usuarios		X
Servidores	X	
Gestión	X	
Oficinas	X	
Internet		X

Tabla 16: Diseño MPLS por entorno

La tabla anterior muestra que los entornos de Usuarios e Internet van a ser entornos locales. Esto quiere decir que sus VLANes no se van a extender entre los CPDs, pero gracias a los protocolos de encaminamiento que se configurarán en el núcleo, van a ser capaces de "*verse*" con el resto de CPDs.

El resto de entornos se extenderán a N2 entre los tres CPDs pareciendo que están en la misma LAN.

VPN N3

Cada uno de los ámbitos en los que se ha separado la nueva infraestructura tendrá una tabla de rutas o VRF independiente; inicialmente todos los ámbitos serán visibles entre ellos y, posteriormente, en función de las necesidades, se definirá o filtrará la visibilidad entre ámbitos.

Las VPN de nivel 3 o VRF que se implementarán en la nueva red son:

- **VPN_SERVIDORES:** Consistirá en la red de acceso de servidores formada por los equipos Catalyst 6509 (*VSS),* conectándose al núcleo mediante doble enlace físico y lógico. Esta VPN utiliza OSPF, como protocolo de encaminamiento con el núcleo.

- **VPN_USUARIOS:** Consistirá en la red de acceso de usuarios formada por los equipos Juniper EX4200-24F conectándose al núcleo mediante doble enlace físico y lógico. Esta VPN utiliza OSPF como protocolo de encaminamiento con el núcleo.

- **VPN_GESTION:** Consistirá en la red de gestión para administrar los equipos de red a través de una red fuera de banda. Se define una VPN para este ámbito. Como protocolo de encaminamiento con el núcleo se utilizan rutas estáticas hacía el *firewall*.

- **VPN_OFICINAS:** Este entorno está formado por los Catalyst 6504 actuales de sucursales localizados en Alcobendas y Leganés, que se enlazarán con un enlace físico y lógico contra los MX480 de cada CPD. Actualmente este ámbito utiliza OSPF como protocolo de encaminamiento con el núcleo, y se mantendrá así durante el proceso de integración.

- **VPN_INTERNET:** El acceso a Internet se realiza de forma redundada por los edificios de Alcobendas y Leganés mediante el proveedor externo. Como protocolo de encaminamiento con el núcleo se utilizan rutas estáticas hacia el *firewall* de Internet, que es el que hace de nivel 3 en este entorno.

Cada uno de los MX480 del núcleo albergará cinco tablas de rutas independientes (una por cada entorno). A continuación se detalla la forma en la que se realiza la configuración en el núcleo:

Para identificar en la nube MPLS los servicios que se anuncian mediante MP-BGP, se define un valor para cada uno de los ámbitos; este valor se utilizará para definir los atributos, *Route-distinguiser* y comunidades (*router-target*) de las *virtual routing forwarding (*VRF).

Servicio	Servidores	Usuarios	Oficinas	Gestión	Internet
ID Servicio	5000	5001	5002	5003	5004

Tabla 17: *route-distinguiser* de cada entorno

Tal y como se ha mencionado antes, para identificar y separar VRF en una nube MPLS se utiliza el atributo *route-distinguiser* (RD). Para identificar el equipo y servicio que realiza los anuncios en la red, se ha elegido el formato "*ip_address:numero*" para el RD, donde la *ip_address* será la dirección de *loopback* de los equipos MX y el número será el *id servicio*.

A continuación se indican el valor del ***Route-Distinguiser*** para todas las VRF de los equipos.

Servicio	RD ALCROC01	RD ALCROC02	RD LEGROC01	RD LEGROC02	RD GETROC01	RD GETROC02
Servidores	172.25.10.241:5000	172.25.10.242:5000	172.25.10.243:5000	172.25.10.244:5000	172.25.10.245:5000	172.25.10.246:5000
Usuarios	172.25.10.241:5001	172.25.10.242:5001	172.25.10.243:5001	172.25.10.244:5001	172.25.10.245:5001	172.25.10.246:5001
Oficinas	172.25.10.241:5002	172.25.10.242:5002	172.25.10.243:5002	172.25.10.244:5002	172.25.10.245:5002	172.25.10.246:5002
Gestión	172.25.10.241:5003	172.25.10.242:5003	172.25.10.243:5003	172.25.10.244:5003	172.25.10.2455003	172.25.10.246:5003
Internet	172.25.10.241:5004	172.25.10.242:5004	172.25.10.243:5004	172.25.10.244:5004	172.25.10.245:5004	172.25.10.246:5004

Tabla 18: *ip_address:route-distinguiser* de cada entorno

Para interconectar las VPN a través de la nube MPLS es necesario disponer del *route-target* definido mediante comunidades extendidas de BGP.

El formato para las *community* es *target:AS_number:id_servicio,* y se utilizará el AS privado 65410.

La siguiente tabla muestra las *community* que exportará cada VRF:

VPN	COMMUNITY EXPORT
Servidores	target:65410:5000
Usuarios	target:65410:5001
Oficinas	target:65410:5002
Gestión	target:65410:5003
Internet	target:65410:5004

Tabla 19: *Communities* de cada entorno

Para que en la misma VPN se tenga conectividad entre CPDs, se ha de importar al menos la misma *community* que exporta.

Para conectar una VPN con otras VPN es necesario importar las *communities* de esas VPN. Por ejemplo, para la que VPN Servidores tenga conectividad con la VPN de Internet, habrá que importar la tabla de la VPN de Internet en la de Servidores. De esa manera, desde Servidores se podrá llegar a Internet ya que la tabla lleva la información necesaria. En un principio, todas las VPNs tendrán visibilidad con el resto.

Para que la solución de interconexión de VPN sea lo más redundante posible, dentro del mismo PE también se interconectan las VPN en función del *import/export* de *community*, con la funcionalidad *auto-export* de Juniper (en los MX480 del núcleo).

A continuación se expone la necesidad de interconectar las VPN dentro del mismo PE.

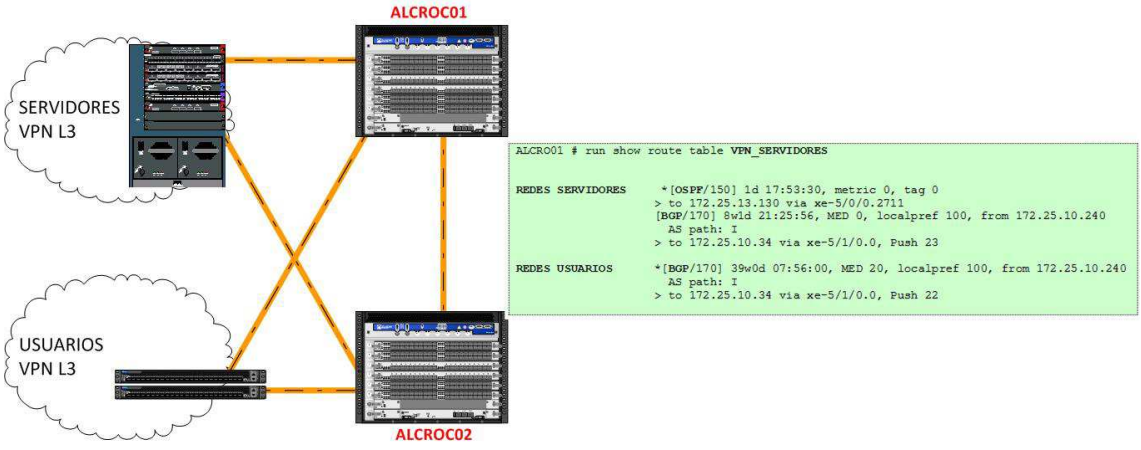


Figura 54: Ejemplo de configuración sin la funcionalidad *auto-export* en un CPD

Según se muestra en la imagen anterior, dentro de un mismo CPD, cada PE dispone de tablas de rutas o VRF independientes para cada ámbito de Distribución; en este ejemplo, Servidores y Usuarios. En el ejemplo de la figura se muestra que las VRF de Servidores y Usuarios están interconectadas entre sí mediante BGP, de forma que la tabla de rutas de la VPN de Servidores en ALCROC01 alcanza las redes de los servidores a través del enlace directo con los 6500 (por OSPF) y a través del enlace directo con ALROC02 (por BGP). Por otro lado, las redes de usuarios únicamente las alcanza a través del anuncio BGP de su pareja de MX (ALCRO02).

En este escenario, aunque la distribución de usuarios disponga de doble enlace con el núcleo, en caso de caída del enlace Dist.Usuarios–ALCRO02, ALCRO01 dejará de alcanzar las redes de usuarios a través de la VRF de servidores, puesto que su vecino deja de anunciarlas.

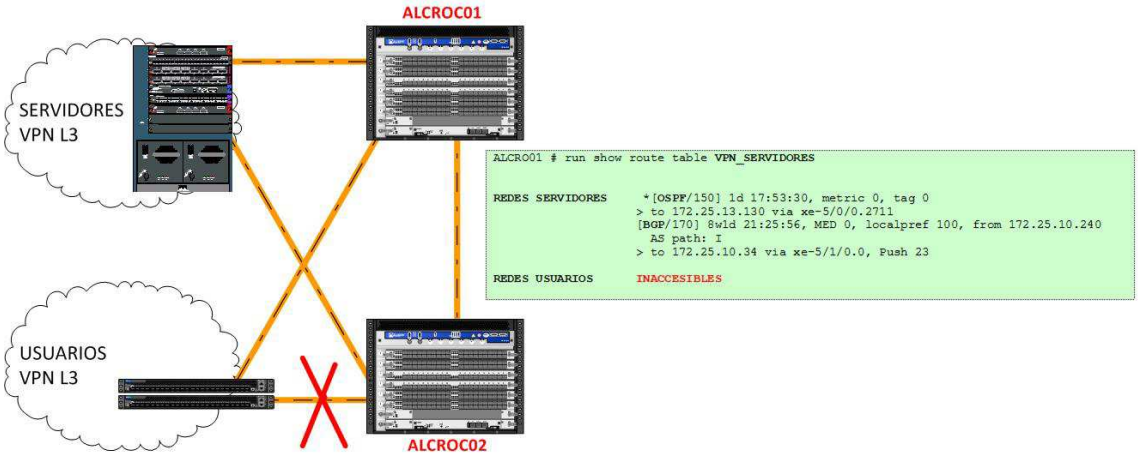


Figura 55: Ejemplo de caída de enlace sin la funcionalidad *auto-export* en un CPD

Tal y como se ha mencionado anteriormente, si se configura la funcionalidad *auto-export* en aquellas VRF que necesiten interconexión con otras VRF dentro de un mismo PE, observamos en la siguiente imagen que la VRF de Servidores alcanza las redes de la VPN del Usuarios a través de la conexión directa Dist.Usuarios-ALCRO01 además de por BGP.

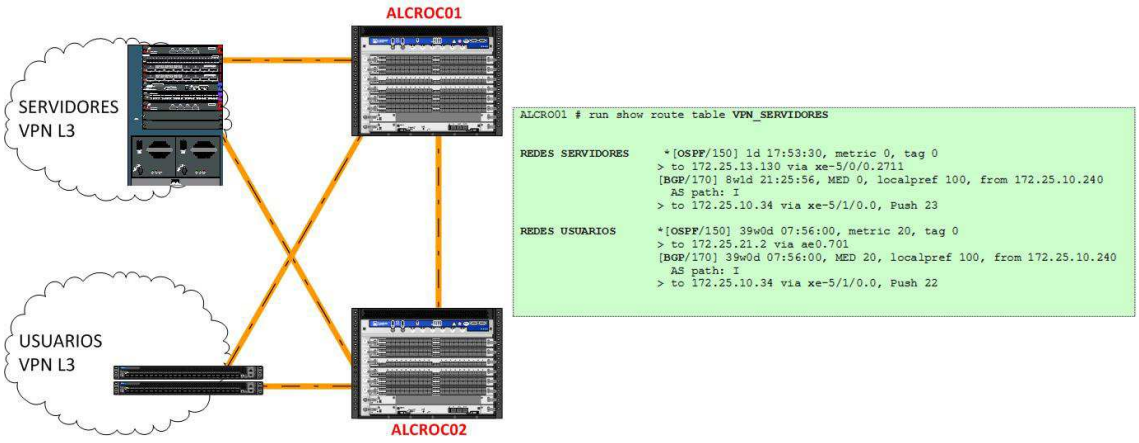


Figura 56: Ejemplo de configuración con la funcionalidad *auto-export* en un CPD

Además de esta configuración, para que aprenda OSPF a través de las distribuciones, habrá que configurar OSPF con área 0 en las VPN de Usuarios y Servidores.

A continuación se exponen la configuración tipo de una VPN de nivel 3, poniendo como ejemplo la VPN de Servidores en el MX1 de Alcobendas (ALCROC01).

```
# POLITICAS PARA IMPORTAR/EXPORTAR COMMUNITY E INTERCONECTAR VPN MEDIANTE MP-BGP y en
LOCAL con AUTO-EXPORT

## Crear las community
```

```
set policy-options community SERVIDORES members target:65412:5000
set policy-options community USUARIOS members target:65412:5001
set policy-options community OFICINAS members target:65412:5002
set policy-options community GESTION members target:65412:5003
set policy-options community INTERNET members target:65412:5004

## Crear políticas para interconectar VPN:

## Se exportan las redes aprendidas por OSPF, estáticas y directamente conectadas

set policy-options policy-statement servidores_export term 1 from protocol ospf
set policy-options policy-statement servidores_export term 1 from protocol direct
set policy-options policy-statement servidores_export term 1 from protocol static
set policy-options policy-statement servidores_export term 1 then community add SERVIDORES
set policy-options policy-statement servidores_export term 1 then accept
set policy-options policy-statement servidores_export term 2 then reject

# Se importan a la VPN de Servidores las redes de servidores aprendidas por BGP (de los
otros MX)
set policy-options policy-statement servidores_import term vrf-servidores from protocol bgp
set policy-options policy-statement servidores_import term vrf-servidores from community SERVIDORES
set policy-options policy-statement servidores_import term vrf-servidores then accept

# Se importan a la VPN de Servidores las redes de oficinas aprendidas por BGP (de los
otros MX)
set policy-options policy-statement servidores_import term vrf-oficinas from protocol bgp
set policy-options policy-statement servidores_import term vrf-oficinas from community OFICINAS
set policy-options policy-statement servidores_import term vrf-oficinas then accept

# Se importan a la VPN de Servidores las redes de usuarios aprendidas por BGP (de los
otros MX)
set policy-options policy-statement servidores_import term vrf-usuarios from protocol bgp
set policy-options policy-statement servidores_import term vrf-usuarios from community USUARIOS
set policy-options policy-statement servidores_import term vrf-usuarios then accept

# Se importan a la VPN de Servidores las redes de gestión aprendidas por BGP (de los
otros MX)
set policy-options policy-statement servidores_import term vrf-gestion from protocol bgp
set policy-options policy-statement servidores_import term vrf-gestion from community EEEE
set policy-options policy-statement servidores_import term vrf-gestion then accept




# Se importan a la VPN de Servidores las redes de internet aprendidas por BGP (de los
otros MX)
set policy-options policy-statement servidores_import term vrf-internet from protocol bgp
set policy-options policy-statement servidores_import term vrf-internet from community INTERNET
set policy-options policy-statement servidores_import term vrf-internet then accept

# Se importan a la VPN de Servidores las redes de oficinas aprendidas localmente (de la
distribución)
set policy-options policy-statement servidores_import term vrf-oficinaslocal from protocol static
set policy-options policy-statement servidores_import term vrf-oficinaslocal from protocol direct
set policy-options policy-statement servidores_import term vrf-oficinaslocal from protocol ospf
set policy-options policy-statement servidores_import term vrf-oficinaslocal from community OFICINAS
set policy-options policy-statement servidores_import term vrf-oficinaslocal then accept

# Se importan a la VPN de Servidores las redes de usuarios aprendidas localmente (de la
distribución)
set policy-options policy-statement servidores_import term vrf-userlocal from protocol static
set policy-options policy-statement servidores_import term vrf-userlocal from protocol direct
set policy-options policy-statement servidores_import term vrf-userlocal from protocol ospf
set policy-options policy-statement servidores_import term vrf-userlocal from community USUARIOS
set policy-options policy-statement servidores_import term vrf-userlocal then accept

# Se importan a la VPN de Servidores las redes de gestión aprendidas localmente (de la
distribución)
set policy-options policy-statement servidores_import term vrf-gestionlocal from protocol static
set policy-options policy-statement servidores_import term vrf-gestionlocal from protocol direct
set policy-options policy-statement servidores_import term vrf-gestionlocal from community EEEE
set policy-options policy-statement servidores_import term vrf-gestionlocal then accept

# Se importan a la VPN de Servidores las redes de internet aprendidas localmente (de la
distribución)
set policy-options policy-statement servidores_import term vrf-internetlocal from protocol static
set policy-options policy-statement servidores_import term vrf-internetlocal from protocol direct
set policy-options policy-statement servidores_import term vrf-internetlocal from community INTERNET
set policy-options policy-statement servidores_import term vrf-internetlocal then accept

set policy-options policy-statement servidores_import term END then reject
```

```
## CONFIGURACIÓN DE VPN DE SERVIDORES

set routing-instances VPN_SERVIDORES instance-type vrf → Se indica que la VPN es de
nivel 3.
set routing-instances VPN_SERVIDORES interface ae0.701 → Se indica la interfaz que
pertenece a esta VPN
set routing-instances VPN_SERVIDORES route-distinguisher 172.25.10.239:5000 → Se
identifican de que PE proceden los anuncios BGP se configura con la "ip de loopback del
PE:idcommunity."
set routing-instances VPN_SERVIDORES vrf-import servidores_import → Se importan redes
de otras VPNs
set routing-instances VPN_SERVIDORES vrf-export servidores_export → Se exportan redes
de otras VPNs
set routing-instances VPN_SERVIDORES vrf-table-label → Para anunciar/exportar en BGP
las redes de esta VPN con VRF-export indicado. SIN ESTE COMANDO LAS REDES DE ESTA VPN NO
SE ANUNCIA POR BGP A LOS PE DE LA NUBE MPLS.

set routing-instances VPN_SERVIDORES routing-options static route 0.0.0.0/0 discard
set routing-instances VPN_SERVIDORES routing-options static route 0.0.0.0/0 no-install
set routing-instances VPN_SERVIDORES routing-options static route 0.0.0.0/0 preference
200 → Para que no aprenda ninguna ruta 0.0.0.0/0 que se anuncie por estáticas
set routing-instances VPN_SERVIDORES routing-options auto-export → Para  interconectar
dentro de mismo PE distintas VPN
set routing-instances VPN SERVIDORES protocols ospf spf-options delay 50
set routing-instances VPN_SERVIDORES protocols ospf export servidores_export_ospf
set routing-instances VPN_SERVIDORES protocols ospf import import_ospf
set routing-instances VPN SERVIDORES protocols ospf area 0.0.0.0 interface ae0.701
interface-type p2p
set routing-instances VPN SERVIDORES protocols ospf area 0.0.0.0 interface ae0.701
priority 255 → Configuración de OSPF area 0 en la interfaz conectada a la distribución
de servidores. Todo lo que se aprende por OSPF se va a importar a esta VPN y se
exportará todo lo que se aprenda de esta VPN.
```

Para el resto de VPNs se deberá configurar de la misma manera. Lo único que variará será el protocolo de encaminamiento que se hable con la distribución. En el ejemplo dado hemos utilizado OSPF como protocolo de encaminamiento, ya que la distribución de servidores también anuncia sus rutas por OSPF.

Para configurar, por ejemplo, la VPN de Gestión, se configurarán rutas estáticas para que se instalen en la VPN:

```
set routing-instances VPN_GESTION routing-options static route SUBRED_GESTION next-hop
172.25.60.254
set routing-instances VPN GESTION routing-options auto-export
```

Esta configuración se tendrá que realizar para cada una de las redes de gestión, ya que el *firewall* (172.25.60.254) no las anuncia y, por tanto, tendremos que configurarlas estáticamente. Al ser pocas las redes a importar, no será un trabajo muy costoso.

Estas redes de gestión serán VLANes nuevas con direccionamiento nuevo. En principio se reservarán dos direccionamientos para la nueva red de gestión de clase C.

Cabe mencionar que, además de las VPNs, hay que configurar en las interconexiones entre los MX del núcleo y las interfaces de *loopback* el modo de encapsulación MPLS.

A continuación se refleja la configuración a realizar en los equipos de núcleo para activar MPLS tomando como ejemplo el MX1 de Alcobendas:

```
# CONFIGURAR INTERFACES


Se configuran el direccionamiento en las interfaces que forma el núcleo de la red.

Se activa las family mpls en las interfaces de interconexión del núcleo para la envío
de paquetes mpls

Los equipos PE añaden las cabeceras MPLS (32 bits) a los paquetes de datos, si el
núcleo tiene fijado el tamaño de MTU estándar (1500 bytes) existe el riesgo descarte de
paquetes en núcleo por ellos se establece en todas las interfaces de conexión del
núcleo un valor de MTU a 9192 bytes.

interfaces {
    xe-5/1/0 {
        mtu 9192;
        unit 0 {
            family inet {
                address 172.25.100.x/30;
            }
            family mpls;
        }
    }
    xe-4/0/0 {
        mtu 9192;
        unit 0 {
            family inet {
                address 172.25.100.x /30;
            }
            family mpls;
        }
    }


# ACTIVAR EL PROTOCOLO MPLS EN LAS INTERFACES DE INTERCONEXIÓN DEL NUCLEO

protocols {
    mpls {
        interface lo0.0;
        interface xe-5/1/0.0;
        interface xe-4/0.0;
    }
```

La configuración para las VPNs de Gestión e Internet (donde el nivel 3 lo realiza el *firewall*) es algo distinto de las del resto. Para unir a nivel de protocolo los *firewall* con el núcleo, se configurará en cada MX y el *firewall* una interfaz de nivel 3, llamadas en Juniper *irb.* De esta manera, las redes de Gestión e Internet se aprenderán a través de rutas estáticas apuntando al *firewall,l* ya que es el que actúa como puerta de enlace de estas redes.

En el resto de entornos, se utilizará OSPF como protocolo de encaminamiento para aprender las rutas entre el núcleo y las distribuciones.

VPN N2 - VPLS

En la siguiente figura se refleja el funcionamiento de VPLS *multihoming*. En los PE o MX de Alcobendas se define el mismo identificador de dispositivo VPLS o *site* (atributo BGP *site-of-origin*), y se establece un PE o MX como primario y otro como respaldo (atributo BGP *local preference*). En los PE de Leganés y Getafe se definen estos atributos de forma simétrica.

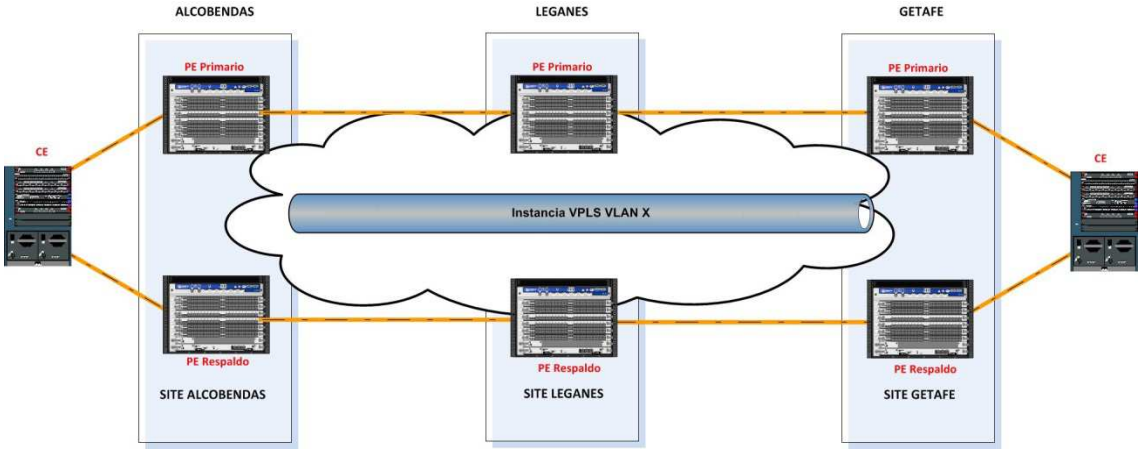


Figura 57: instancia VPLS a lo largo de los CPDs

Según se muestra en la figura anterior, un PE tiene activa la instancia VPLS mientras que en el otro está en modo respaldo. La conexión del CE con el PE de respaldo sólo cursará tráfico en caso de caída de la otra interfaz o del PE primario. De esta forma se tiene que, aunque los CE de los tres CPDs dispongan de doble conexión con el PE, sólo se utilizará una de ellas, evitando así la posibilidad de generar bucles en la red y de configurar *spanning tree*.

Para tener activas ambas interfaces de conexión entre cada distribución y el Núcleo (CE-PE), optimizando así el ancho de banda disponible, se balancearán entre los PE de un mismo *site* las instancias VPLS de las VLANes de Servidores, Oficinas, Gestión, Internet y Usuarios.

Identificación y Configuración instancias VPLS

Para propagar el nivel 2 entre CPDs se va emplear el servicio VPLS. Para aislar al máximo posible los dominios de *broadcast*, uno de los requerimientos solicitados en el proyecto, cada VLAN se propagará mediante una instancia de VPLS diferente.

La señalización o establecimiento de las instancias VPLS entre los PE de la red MPLS, se realiza a través de MP-BGP; y, al igual que para las VPN de nivel 3, es necesario definir el *router -distinguiser* así como el *route-target* con las *community* que importa/exporta cada instancia VPLS.

Los identificadores de las VLANs de Usuarios y Servidores difieren entre los CPDs, por lo que no habrá problema a la hora de extender las VLANes, ya que no se producirá solapamiento.

Las VLANes que se utilizan para hablar OSPF sí tienen el mismo ID en los CPDs, pero no supondrá ningún problema, ya que no se extenderán a N2.

El criterio para definir el fomato del *route-distinguiser* de las VPLS es ***Ip_loopback:id_vlan***. A modo de ejemplo se refleja el RD para la instancia VPLS de la VLAN 50:

Servicio	VLAN_ID	RD ALCROC01	RD ALCROC02	RD LEGCOR01	RD LEGCOR02	RD GETCOR01	RD GETCOR02
VPLS50	50	172.25.10.241:50	172.25.10.242:50	172.25.10.243:50	172.25.10.244:50	172.25.10.243:50	172.25.10.244:50

Tabla 20: *route-distinguiser* para la instancia VPLS con ID 50

El criterio para definir las *community* de las instancias VPLS es ***target:AS_number:id_vlan***

Por ejemplo, para la VLAN 50 la *community* será:

Servicio	VLAN_ID	COMMUNITY export
VPLS50	50	target:65410:50

Tabla 21: *community* para la instancia VPLS con ID 50

Puesto que entre CPDs las instancias VPLS sólo han de tener visibilidad con su misma instancia VPLS, la *community* que se importa y se exporta ha de ser la misma en todos los PEs. A modo de ejemplo se refleja la *community* a importar/exportar para la instancia VPLS50.

A continuación se expone la configuración tipo de una VPN de nivel 2. Las configuraciones definitivas a aplicar en cada uno de los ámbitos se reflejan en los correspondientes apartados de este documento.

```
# CONFIGURACIÓN DE INSTANCIA VPLS PARA LA VLAN 50 DEL AMBITO DE GESTION

Este ejemplo configura la instancia VPLS para que el camino principal entre MX1
ALCOBENDAS → MX1 LEGANES → MX1 GETAFE.

Para que la instancia de VPLS se establezca entre los cuatro PE todas la instancias han
de tener el mismo vrf-target para la misma VPLS. (vrf-target target:65412:50).

Para configurar el VPLS multihoming el site identifier de los PE del mismo CPD ha de ser
igual, se configura a los PE de ALCOBENDAS con site-identifier 1, y en LEGANES con site-
identifier 2 y a los PE de GETAFE con site-identifier 3.

Con el site-range se identifica el número de PE que forman parte de la instancia. Se
configura con valor site-range 6 en todos los PE puesto que cada instancias va a tener
cuatro PE (ALCROC01, ALCROC02, GETROC01, GETROC02, LEGCOR01 y LECROC02)



## Configuración en ALCROC01

routing-instances {
    VPLS50 {
        instance-type vpls; → Se indica que es una instancias VPLS
        vlan-id 50; → Indica el vlan-id de la instancia VPLS
        interface ge-5/0/1.50; → Indica la interfaz que pertenece a esta instancia
        route-distinguisher 172.25.10.241:50; → Identifica quien origina el anuncio en
BGP se configura con la "ip de loopback del PE:id_vlan"
        vrf-target target:65412:50; → Indica que importa/exporta en esta VPLS
        protocols { → Se define el protocolo VPLS en esta instancia
            vpls {
                site-range 6;
                no-tunnel-services; → Permite que se cree de forma dinámica la
interface logica lsi (label-switch-interface) que se utiliza para el intercambio de
etiquetas de VPN. SIN ESTE COMANDO LA INSTANCIA VPLS NO SE ANUNCIA POR BGP A LOS PE DE
LA NUBE MPLS.
                site ALCROC01 { → Se define el site
                    site-identifier 1;
                    multi-homing; → Se define el site como multihomming
                    site-preference primary; → Se define como site pricipal
                    interface ge-5/0/1.50; → Se define la interface
```

```
                }
            }
        }
    }
```

Configuración en ALCROC02

```
routing-instances {
    VPLS50 {
        instance-type vpls;
        vlan-id 50;
        interface ge-5/0/1.50;
        route-distinguisher 172.25.10.242:50;
        vrf-target target:65412:50;
        protocols {
            vpls {
                site-range 6;
                no-tunnel-services;
                site ALCROC02 {
                    site-identifier 1;
                    multi-homing;
                    site-preference backup; → Se define como PE de respaldo.
                    interface ge-5/0/1.50;
                }
            }
        }
    }
```

Configuración en LEGROC01

```
routing-instances {
    VPLS50 {
        instance-type vpls;
        vlan-id 50;
        interface ge-5/0/1.50;
        route-distinguisher 172.25.10.243:50
        vrf-target target:65412:50;
        protocols {
            vpls {
                site-range 6;
                no-tunnel-services;
                site LEGROC01 {
                    site-identifier 2;
                    multi-homing;
                    site-preference primary;
                    interface ge-5/0/1.50;
                }
            }
        }
    }
```

Configuración en LEGROC02

```
routing-instances {
    VLAN50{
        instance-type vpls;
        vlan-id 50;
        interface ge-5/0/1.50;
        route-distinguisher 172.25.10.244:50;
        vrf-target target:65412:50;
        protocols {
            vpls {
                site-range 6;
                no-tunnel-services;
                site LECROC02 {
                    site-identifier 2;
                    multi-homing;
                    site-preference backup;
                    interface ge-5/0/1.50;
}
            }
        }
    }
```

Configuración en GETROC01

```
routing-instances {
    VPLS50 {
        instance-type vpls;
        vlan-id 50;
        interface ge-5/0/1.50;
        route-distinguisher 172.25.10.245:50
        vrf-target target:65412:50;
        protocols {
            vpls {
                site-range 6;
                no-tunnel-services;
                site GETROC01 {
                    site-identifier 3;
                    multi-homing;
                    site-preference primary;
                    interface ge-5/0/1.50;
                }
            }
        }
    }
```

Configuración en GETROC02

```
routing-instances {
    VLAN50{
        instance-type vpls;
        vlan-id 50;
        interface ge-5/0/1.50;
        route-distinguisher 172.25.10.246:50;
        vrf-target target:65412:50;
        protocols {
            vpls {
                site-range 6;
                no-tunnel-services;
                site GETROC02 {
                    site-identifier 3;
                    multi-homing;
                    site-preference backup;
                    interface ge-5/0/1.50;
}
            }
        }
    }
```

De esta manera ya se tiene configurado cada VLAN que se quiere extender a través de los CPDs.

Este diseño ha sido pensado de tal manera que los MX1 de cada CPD conmuten el tráfico de las VLANes pares y hagan de respaldo para las VLANes impares, y los MX2 de cada CPD conmuten el tráfico de las VLANes impares y hagan de respaldo para las VLANes pares. De esta manera se optimiza el ancho de banda de las interconexiones

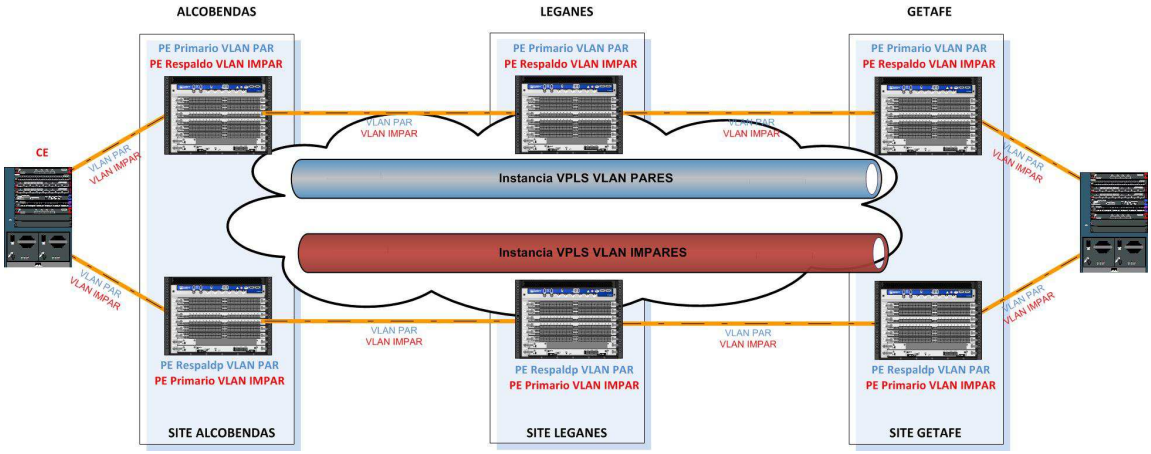


Figura 58: Instancias VPLS pares e impares a lo largo de los CPDs

Filtrado de BPDU a través de VPLS

Para independizar los ámbitos de *Spanning-tree* por CPD, de forma que un cambio topológico en uno de los CPD no afecte al otro, se aplican filtros en cada una de las instancias VPLS que se propagan por el núcleo MPLS.

A continuación se reflejan la configuración de estos filtros:

```
# CONFIGURACIÓN FILTRADO STP

set firewall family vpls filter CONTROL-FLOODING term STP from destination-mac-address
01:80:c2:00:00:00/48
set firewall family vpls filter CONTROL-FLOODING term STP then count STP
set firewall family vpls filter CONTROL-FLOODING term STP then discard
set firewall family vpls filter CONTROL-FLOODING term ALTERNATE-STP from destination-
mac-address 01:80:c2:00:00:00/44
set firewall family vpls filter CONTROL-FLOODING term ALTERNATE-STP then count
ALTERNATE-STP
set firewall family vpls filter CONTROL-FLOODING term ALTERNATE-STP then discard
set firewall family vpls filter CONTROL-FLOODING term PVST from destination-mac-address
01:00:0c:cc:cc:cd/48
set firewall family vpls filter CONTROL-FLOODING term PVST then count PVST
set firewall family vpls filter CONTROL-FLOODING term PVST then discard
set firewall family vpls filter CONTROL-FLOODING term CDP from destination-mac-address
01:00:0c:cc:cc:cc/48
set firewall family vpls filter CONTROL-FLOODING term CDP then count CDP
set firewall family vpls filter CONTROL-FLOODING term CDP then discard
set firewall family vpls filter CONTROL-FLOODING term VLAN-BRIDGE from destination-mac-
address 01:00:0c:cd:cd:ce/48
set firewall family vpls filter CONTROL-FLOODING term VLAN-BRIDGE then count VLAN-BRIDGE
set firewall family vpls filter CONTROL-FLOODING term VLAN-BRIDGE then discard
set firewall family vpls filter CONTROL-FLOODING term STP UPFAST from destination-mac-
address 01:00:0c:cd:cd:cd/48
set firewall family vpls filter CONTROL-FLOODING term STP UPFAST then count STP UPFAST
set firewall family vpls filter CONTROL-FLOODING term STP UPFAST then discard
set firewall family vpls filter CONTROL-FLOODING term CGMP from destination-mac-address
01:00:0c:dd:dd:dd/48
set firewall family vpls filter CONTROL-FLOODING term CGMP then count CGMP
set firewall family vpls filter CONTROL-FLOODING term CGMP then discard
set firewall family vpls filter CONTROL-FLOODING term ISL from destination-mac-address
01:00:0c:00:00:00/48
set firewall family vpls filter CONTROL-FLOODING term ISL then count ISL
set firewall family vpls filter CONTROL-FLOODING term ISL then discard
set firewall family vpls filter CONTROL-FLOODING term DEFAULT then accept

# APLICAR FILTRO A LA INSTANCIA VPLS
```

```
set routing-instances VPLS50 forwarding-options family vpls flood input CONTROL-FLOODING
```

Lo que hace, básicamente, este filtro es filtrar protocolos de red para que no se propaguen a lo largo de los CPDs. Los protocolos que no se deben propagar para evitar bucles innecesarios son *spanning-tree* (STP o PVST), *Cisco Discovery Protocol* (CDP), *Cisco Group Management Protocol* (CGMP) y *Cisco Inter-switch Link* (ISL). Para identificar cada uno de estos protocolos, se utilizan MACs dedicadas a ello; basta con configurar el filtro basándose en estas MACs para saber qué se debe filtrar en cada instancia VPLS.

5.3.3 Configuración de OSPF

Para todos los equipos del núcleo se configurarán rutas estáticas que serán la base para poder establecer las sesiones IBGP que se formarán para la señalización del VPLS *multihoming* comentado en los anteriores apartados.

Se utilizarán para alcanzar las direcciones de *loopback* de los equipos del núcleo a través de la línea de interconexión del operador.

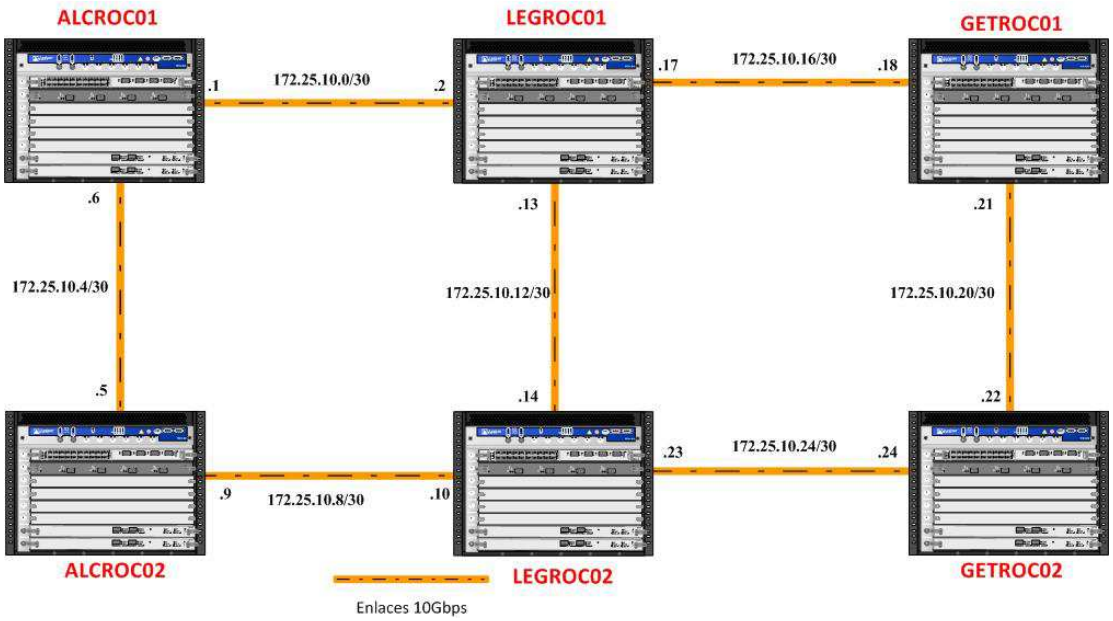


Figura 59: Esquema final OSPF a lo largo de los CPDs

Estas rutas se redistribuirán en el protocolo interior (OSPF) de cada entidad para proporcionar la redundancia. En caso de caída de la línea del operador, el equipo podrá alcanzar a la entidad remota a través del equipo redundante de su propio CPD. El OSPF del núcleo se configura como área 0 para todas las *interfaces* de los equipos del núcleo.

La configuración de las rutas estáticas se basa en la siguiente filosofía:

- La ruta desde un CPD a otro con el que tenga conexión directa, tendrá distancia administrativa 1.
- La ruta desde un CPD a otro con el que no tenga conexión directa, tendrá distancia administrativa 200.

- Además, se redistribuirán estas rutas estáticas a OSPF. De esta forma, OSPF tendrá conocimiento de estas rutas y habrá conexión entre los equipos que no tengan conectividad directa.

Para mejorar la convergencia de OSPF en caso de caída de *interfaces*, se activa el protocolo BFD (*Bidirectional Forwarding Detection*) que es capaz de detectar rápidamente la caída y ajustar el SPF *delay* para acelerar su reconvergencia.

A continuación se refleja la configuración a realizar, tomando como ejemplo el MX ALCROC01:

```
# CONFIGURACIÓN OSPF

Establecer Router-ID: se toma la dirección de loopback.

routing-options {
    router-id 172.25.10.239;
        }

Se activa OSPF en las interfaces de Interconexión del núcleo

protocols {
ospf {
        spf-options {
            delay 50;
        }
        area 0.0.0.0 {
            interface xe-5/1/0.0 { → Conexión contra LEGROC01
                bfd-liveness-detection {  → Se activa a BFD para mejorar los tiempos de
convergencia
                    minimum-interval 100;
                }
            }
            interface xe-4/0/0.0 { → Conexión contra ALCROC02
                bfd-liveness-detection {
                    minimum-interval 100;
                }
            }

            interface lo0.0; → Se anuncia por OSPF la loopback. Necesario para el
funcionamiento de BGP, puesto que la señalización de MPLS se realiza con la interfaz de
loopback.
        }
    }
```

5.3.4 Configuración de BGP

Se activa en los equipos del núcleo la extensión de BGP denominada *Multiprotocol* BGP (MP-BGP), que permite el transporte de NLRI para la señalización de las instancias VPLS y de las VPN de nivel 3.

A continuación se describe la configuración BGP a implementar, tomando como referencia el MX1 de Alcobendas:

```
# CONFIGURACIÓN DE BGP EN ALCROC01
```

```
protocols {
        bgp {
        group interno {   → Se configura el grupo BGP
            type internal; → Se indica que las sesiones son iBGP
            local-address 172.25.10.241; → Se establece la ip de loopback para
establecimiento de las sesiones
            family inet {
                unicast;
            }
            family inet-vpn { → Se active MP-BGP para el transporte NRLI de VPN N3
                unicast;
            }
            family l2vpn { → Se active MP-BGP para el transporte NRLI de VPLS
                signaling;
            }
            local-as 65412; → Se definen el AS

            Se definen los vecinos BGP:
            neighbor 172.25.10.242;
            neighbor 172.25.10.243;
            neighbor 172.25.10.244;
            neighbor 172.25.10.245;
            neighbor 172.25.10.246;

        }
    }
```

5.3.5 Definición de VLANes y VRRP

A continuación se expone el listado completo del direccionamiento e identificadores de VLANes que existen actualmente en las dos empresas:

	LEGANÉS		ALCOBENDAS		GETAFE	
	IP	VLAN ID	IP	VLAN ID	IP	VLAN ID
SERVIDORES	172.18.1.0/24	1000	172.18.4.0/24	1000	172.16.3.0/24	40
	172.18.2.0/24	1001	172.18.5.0/24	1001		
	172.18.3.0/24	1002	172.18.6.0/24	1002		
USUARIOS_DATOS	172.20.1.0/24	2000	172.20.4.0/24	2000	10.10.10.0/24	10
	172.20.2.0/24	2001	172.20.5.0/24	2001	10.10.11.0/24	11
	172.20.3.0/24	2002	172.20.6.0/24	2002		
USUARIOS_VOZ	172.21.1.0/24	2000	172.21.4.0/24	2000	10.10.30.0/24	30
	172.21.2.0/24	2001	172.21.5.0/24	2001	10.10.31.0/24	31
	172.21.3.0/24	2002	172.21.6.0/24	2002		
OFICINAS	10.0.0.0/8		10.0.0.0/8			
GESTIÓN	172.16.1.0/24	100	172.16.2.0/24	101	10.10.50.0/24	50
INTERNET	172.30.1.0/24	3000	172.30.1.0/24	3000	172.30.1.0/24	3000

Tabla 22: direccionamiento después de la integración

Observando la tabla 22, se puede apreciar claramente que los identificadores de las VLANes en los CPDs de Leganés y Alcobendas coinciden en los entornos de Servidores y Usuarios. Antes de la integración, que los ID de las VLANes coincidiesen no era ningún problema, ya que eran VLANes locales y nunca se tuvo en cuenta una posible extensión de las mismas a través de los CPDs en el futuro, por lo que ahora conlleva a un solapamiento de las mismas.

Como ejemplo, diremos que el servidor A en la VLAN 1000 en el CPD de Leganés, necesita comunicarse con el servidor B en la VLAN 1000 en el CPD de Alcobendas. Al ser una comunicación de N3 (los direccionamientos no son los mismos), cuando el paquete de información llegue a la distribución, verá que aprende la ruta a través del núcleo, por lo que enviará el paquete al núcleo. El núcleo tendrá que etiquetar este paquete para encapsularlo en un paquete VPLS. Aquí es donde existe solapamiento. La etiqueta con el ID 1000 lo aprenden por ambos CPDs, y no sabría si enviarlo de nuevo hacia su distribución local o al MX remoto.

Para solucionar este problema, se cambiarán los IDs de ls VLANes de la red de servidores del CPD de Alcobendas por las siguientes:

	ALCOBENDAS	
	IP	VLAN ID
SERVIDORES	172.18.4.0/24	1003
	172.18.5.0/24	1004
	172.18.6.0/24	1005
USUARIOS_DATOS	172.20.4.0/24	2006
	172.20.5.0/24	2007
	172.20.6.0/24	2008
USUARIOS_VOZ	172.21.4.0/24	2009
	172.21.5.0/24	2010
	172.21.6.0/24	2011

Tabla 23: VLAN IDs nuevas en Alcobendas para evitar el solapamiento

En cuanto al direccionamiento, se puede contemplar que las subredes de Getafe entran en el rango de oficinas de Alcobendas y Leganés, por lo que existiría aquí un solapamiento a nivel de direccionamiento. Existen dos opciones para solventar el problema:

- La instalación de un *firewall* en Getafe que realice traducción de direccionamiento (o *Network Address Translation* – NAT). De esta manera, cada entorno de Getafe se traduciría por una subred privada que no se solapase con ninguna de los otros dos CPDs. Esta sería la solución más rápida a implementar, aunque no la más sencilla, ya que puede conllevar fallos en la configuración del *firewall* y provocar malfuncionamientos en la red.

- La otra opción, que realizaremos a petición de cliente, será cambiar el direccionamiento de la red de Getafe por otro que no se esté utilizando.

Además de su extensión a N2 mediante VPLS, las distribuciones utilizarán VRRP para dar redundancia de puerta de enlace a cada una de las VLANes. Para cada una de ellas, VRRP se define de la siguiente manera:

				IPs FÍSICAS - PRIORIDAD VRRP			
	VLAN ID	SUBRED	IP VIRTUAL	LEGANES	ALCOBENDAS	GETAFE	VRRP Group
SERVIDORES	1000	172.18.1.0/24	172.18.1.8	172.18.1.9 - 255	172.18.1.10 - 253	172.18.1.11 - 254	100
	1001	172.18.2.0/24	172.18.2.8	172.18.2.9 - 255	172.18.2.10 - 253	172.18.2.11 - 254	101
	1002	172.18.3.0/24	172.18.3.8	172.18.3.9 - 255	172.18.3.10 - 253	172.18.3.11 - 254	102
	1003	172.18.4.0/24	172.18.4.8	172.18.4.9 - 253	172.18.4.10 - 255	172.18.4.11 - 254	103
	1004	172.18.5.0/24	172.18.5.8	172.18.5.9 - 253	172.18.5.10 - 255	172.18.5.11 - 254	104
	1005	172.18.6.0/24	172.18.6.8	172.18.6.9 - 253	172.18.6.10 - 255	172.18.6.11 - 254	105
	40	172.22.0.0/24	172.22.0.8	172.22.0.9 - 254	172.22.0.10 - 253	172.22.0.11 - 255	106
USUARIOS_DATOS	2000	172.20.1.0/24	172.20.1.8	172.20.1.9 - 255	172.20.1.10 - 253	172.20.1.11 - 254	107
	2001	172.20.2.0/24	172.20.2.8	172.20.2.9 - 255	172.20.2.10 - 253	172.20.2.11 - 254	108
	2002	172.20.3.0/24	172.20.3.8	172.20.3.9 - 255	172.20.3.10 - 253	172.20.3.11 - 254	109
	2006	172.20.4.0/24	172.20.4.8	172.20.4.9 - 253	172.20.4.10 - 255	172.20.4.11 - 254	110
	2007	172.20.5.0/24	172.20.5.8	172.20.5.9 - 253	172.20.5.10 - 255	172.20.5.11 - 254	111
	2008	172.20.6.0/24	172.20.6.8	172.20.6.9 - 253	172.20.6.10 - 255	172.20.6.11 - 254	112
	10	172.22.1.0/24	172.22.1.8	172.22.1.9 - 254	172.22.1.10 - 253	172.22.1.11 - 255	113
	11	172.22.2.0/24	172.22.2.8	172.22.2.9 - 254	172.22.2.10 - 253	172.22.2.11 - 255	114
USUARIOS_VOZ	2003	172.21.1.0/24	172.21.1.8	172.21.1.9 - 255	172.21.1.10 - 253	172.21.1.11 - 254	115
	2004	172.21.2.0/24	172.21.2.8	172.21.2.9 - 255	172.21.2.10 - 253	172.21.2.11 - 254	116
	2005	172.21.3.0/24	172.21.3.8	172.21.3.9 - 255	172.21.3.10 - 253	172.21.3.11 - 254	117
	2009	172.21.4.0/24	172.21.4.8	172.21.4.9 - 253	172.21.4.10 - 255	172.21.4.11 - 254	118
	2010	172.21.5.0/24	172.21.5.8	172.21.5.9 - 253	172.21.5.10 - 255	172.21.5.11 - 254	119
	2011	172.21.6.0/24	172.21.6.8	172.21.6.9 - 253	172.21.6.10 - 255	172.21.6.11 - 254	120
	30	172.22.3.0/24	172.22.3.8	172.22.3.9 - 254	172.22.3.10 - 253	172.22.3.11 - 255	121
	31	172.22.4.0/24	172.22.4.8	172.22.4.9 - 254	172.22.4.10 - 253	172.22.4.11 - 255	122
GESTIÓN	50	172.16.1.0/24	172.16.1.8	172.16.1.9 - 255	172.16.1.10 - 253	172.16.1.11 - 254	123
INTERNET	3000	172.30.1.0/24	172.30.1.8	172.30.1.9 - 255	172.30.1.10 - 253	172.30.1.11 - 254	124

Tabla 24: Direccionamiento VRRP después de la integración

Tal y como se muestra en la Tabla 24, el *master* de cada grupo VRRP será aquel cuyo CPD ya tenía la VLAN albergada antes de la integración de los tres CPDs. El motivo por el que se han elegido estas prioridades (*masters*/*backups*) es para que el tráfico no dé vueltas innecesarias, procurando tener el N3 localmente según las necesidades de cada VLAN. También es una buena forma de repartir el tráfico por igual en los CPDs primarios (Leganés y Alcobendas). El

backup será para todas, excepto para la suya propia, la distribución de Getafe, ya que al ser el CPD más pequeño en cuanto a tráfico a procesar, será el más óptimo para llevar el encaminamiento de estas VLANes en caso de que el *master* caiga.

6. PLANIFICACIÓN Y PRESUPUESTO

En el presente anexo se estiman los costes de desarrollo del Proyecto de Integración. Se tendrán en cuenta tanto los costes de servicio como los de *hardware* y *software*.

En cuanto a los costes de servicio, se considerarán:

- Dirección del proyecto: coordinación y seguimiento durante el desarrollo del proyecto.
- Documentación de la tecnología empleada.
- Definición de requisitos durante el ciclo de vida del proyecto.
- Diseño de toda la infraestructura de red.
- Diseño de la configuración de todo el equipamiento a utilizar.
- Plan de pruebas y homologación de cada una de las infraestructuras a implementar, incluyendo las configuraciones de los equipos.
- Instalación física de los componentes de red en los CPDs y en los cuartos técnicos de las plantas.
- Instalación del cableado estructurado, tanto de cobre como fibra óptica.
- Pruebas finales una vez instalada toda la infraestructura de red de los tres CPDs.
- Documentación final del proyecto.

El equipo que implementará el proyecto estará formado por un ingeniero superior y tres ingenieros técnicos. Estimando que los honorarios de cada uno son 90 €/hora y 60 €/hora, respectivamente.

Actividad	Jornadas		Precio (€)
Dirección del proyecto	Ing. Superior	10	7200
	Ing. Técnico	5	2400
Definición de requisitos	Ing. Superior	5	3600
	Ing. Técnico	5	2400
Diseño de la arquitectura de red	Ing. Superior	10	7200
Diseño de la configuración de componentes *hardware*	Ing. Técnico	15	7200
Instalación física del *hardware*	Ing. Técnico	20	9600
Realización del plan de pruebas	Ing. Técnico	5	2400
Pruebas de la arquitectura de red	Ing. Técnico	5	2400
Reajuste y evaluación final	Ing. Técnico	5	2400
Documentación final del proyecto	Ing. Superior	10	7200
	Ing. Técnico	5	2400
Total		**100**	**56400**

Tabla 25: Costes de recursos humanos

Los costes relacionados con la electrónica incluida en el diseño final de la arquitectura de red, incluyendo el soporte *hardware/software* por parte del fabricante, son los siguientes:

CONCEPTO		PRECIO (€)
Juniper MX480	**Módulo**	
Chasis		3000
Slot 4	DPCE-R-20GE-4XGE	90000
Slot 5	DPC-R-4XGE-XFP:	72000
Fuente 1	MX480BASE3-AC	2000
Fuente 2	MX480BASE3-AC	2000
	Unidades: 2	**338000**
Catalyst 6509		
Chasis		
Slot 1	WS-X6708-10GE	30000
Slot 2	WS-X6724-SFP	26000
Slot 3	WS-X6708-10GE	30000
Slot 4	VS-S720-10G	28000
Slot 5	VS-S720-10G	28000
Slot 6	WS-X6748-GE-TX	22000
Fuente 1		3500
Fuente 2		3500
	Unidades:4	**663000**
Catalyst 3750X-48P		12000
Fuente redundante		1500
Cable stack		250
	Unidades: 20	**275000**
Juniper EX4200-48T		8000
Fuente redundante		1000
Cable stack		180
	Unidades: 44	**403920**
Juniper EX4200-24F		15000
Fuente redundante		1000
Cable stack		180
	Unidades: 12	**194160**
Fortigate 1240B		24000
	Unidades: 5	**120000**
	TOTAL	**1656080**

Tabla 26: Costes de equipamiento *hardware*

Costes totales:

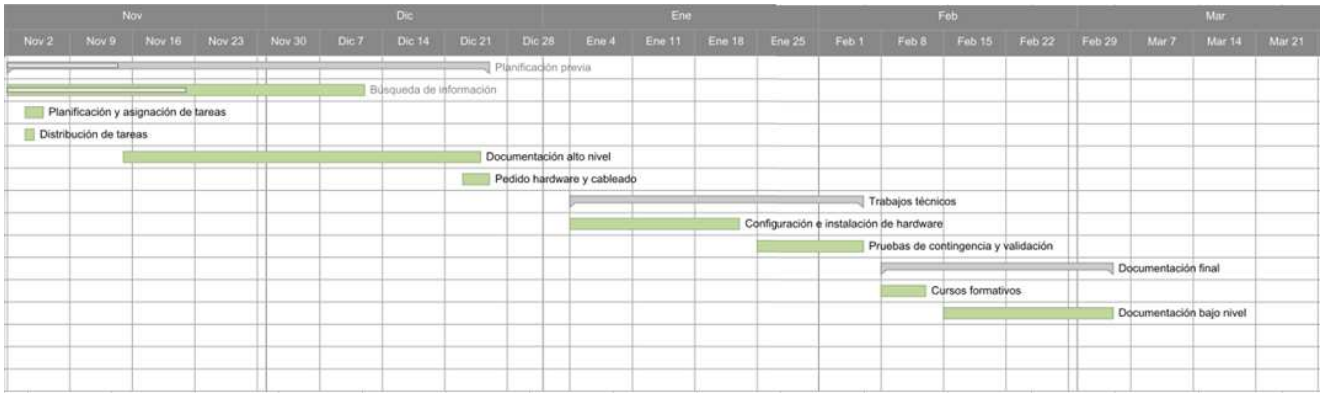
Sumando todos los costes resulta el coste final del proyecto:

CONCEPTO	PRECIO (€)
Recursos Humanos	**564 000**
Equipamiento *hardware*	**1 656 080**
TOTAL	**2 220 080**

Tabla 27: Coste total de proyecto

Diagrama de Gantt:

	Nombre de la tarea	Fecha de inicio	Fecha de finalización	Duración
1	Planificación previa	02/11/15	25/12/15	40d
2	Búsqueda de información	02/11/15	11/12/15	30d
3	Planificación y asignación de tareas	04/11/15	05/11/15	2d
4	Distribución de tareas	04/11/15	04/11/15	1d
5	Documentación alto nivel	15/11/15	24/12/15	30d
6	Pedido hardware y cableado	23/12/15	25/12/15	3d
7	Trabajos técnicos	04/01/16	05/02/16	25d
8	Configuración e instalación de hardware	04/01/16	22/01/16	15d
9	Pruebas de contingencia y validación	25/01/16	05/02/16	10d
10	Documentación final	08/02/16	04/03/16	20d
11	Cursos formativos	08/02/16	12/02/16	5d
12	Documentación bajo nivel	15/02/16	04/03/16	15d
13				
14				
15				



7. CONCLUSIONES Y TRABAJOS FUTUROS

El objetivo de este proyecto es el de proveer de conectividad a las dos empresas recién fusionadas, dotándolas de alta disponibilidad, fácilmente gestionable y actualizable, y con un mínimo impacto en su crecimiento, siguiendo el modelo de red de 3 capas.

La situación actual de la empresa C presenta un diseño de red que no se corresponde a un centro de datos como tal y en el que se encuentran todos los niveles colapsados en su equipo central. Este diseño impide un crecimiento de la red donde no exista un impacto importante sobre el resto de su electrónica. No permite diferenciar bloques o equipos cuyas funcionalidades sean claramente identificadas (a la hora de poder segmentar la red).

El diseño que se ha propuesto para los tres CPDs de la empresa C y G ofrecen todas las posibilidades y características que debe tener un centro de datos hoy en día: redundancia, alta disponibilidad, ancho de banda, diseño distribuido, modularidad, gestionable fácilmente, etc.

La distribución de las distintas VLANes se ha realizado de manera que quedase totalmente diferenciada la funcionalidad de los equipos que iban a contener.

Un centro de datos exige, además, que todas las comunicaciones sean lo más fluidas posibles. Por este motivo, los enlaces entre los equipos a través de los diferentes niveles del CPD son de 10Gbps. Estos *uplinks*, son lo que ofrecen mayor ancho de banda disponible en la actualidad, reduciendo la latencia considerablemente en aplicaciones con gran volumen de tráfico, como *backups* realizados regularmente.

La nueva infraestructura integrada se ha diseñado pensando en el futuro. Esto quiere decir que si se quiere ampliar la red dotándolo de un nuevo servicio o entorno, se conectará directamente al bloque del núcleo para no perder el diseño de tres niveles.

Si lo que se quiere es ampliar equipos porque o bien se hayan quedado obsoletos o bien se ha llegado al límite de utilización de puertos, basta con actualizar los chasis o ampliar las pilas de Cisco o Juniper.

Una red tan grande como la que resulta de la integración de estas dos empresas, debe ser monitorizada a gran escala y por un *software* capaz de soportar todos los equipos que la componen, como la herramienta *Spectrum* o *Nagios*.

Se recomienda realizar *backups* semanales de todos los equipos de la red, ya sea manual o automáticamente, por alguna herramienta SNMP, por ejemplo.

Un importante trabajo futuro a tener en cuenta será la de dotar al entorno Core de alta disponibilidad de enlaces. Para ello, es recomendable realizar una interconexión completamente mallada donde haya enlaces directos entre todos los equipos que componen el núcleo.

El estudio de viabilidad y cobertura de la tecnología Wi-Fi (*Wireless Fidelity*) podría aportar al proyecto otro servicio de valor añadido al usuario final, dotando de movilidad y capacidad de acceso a los recursos de la red desde cualquier lugar dentro de las instalaciones de las dos empresas.

Bibliografía

[1] *Cisco Systems Inc. – Data Center Network Infraestructure*. URL:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/ns304/networking_solutions_package.html

[2] *Cisco Systems Inc. – Cisco Catalyst 6500 and 6500-E Series Switch Data Sheet.* URL:

http://cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[3] *Cisco Systems Inc. – VRRP.* URL:

http://www.cisco.com/c/en/us/support/docs/security/vpn-3000-series-concentrators/7210-vrrp.html

[4] *Cisco Systems Inc. – Virtual Switching Systems (VSS).* URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vss.html

[5] *Cisco Systems Inc. – Cisco StackWise.* URL:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html

[6] *Cisco Systems Inc. – IEEE 802.1Q Frame Format.* URL:

http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html

[7] *Cisco Systems Inc. – Link Aggregation Control Protocol (*LACP). URL:

http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html

[8] *Cisco Systems Inc. – MPLS Fundamentals.* URL:

http://www.ciscopress.com/store/mpls-fundamentals-9781587051975

[9] *Juniper Networks – EX4200 Technical Documentation.* URL:

http://www.juniper.net/us/en/products-services/switching/ex-series/ex4200/

[10] *Juniper Networks – MX480 Technical Documentation.* URL:

http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/chassis-mx480-description.html

[11] *Juniper Networks – Virtual Chassis Documentation.* URL:

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/virtual-chassis-ex4200-components.html

[12] *Juniper Networks – VPN routing-instances configuration.* URL:

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/routing-instances-overview.html

[13] *Juniper Networks – VPLS Configuration Guide.* URL:

http://www.juniper.net/techpubs/en_US/junos12.3/information-products/pathway-pages/config-guide-vpns/config-guide-vpns-vpls.html